

ALGORITHMS AND CLASSIFICATION IN GROUPS OF PIECEWISE-LINEAR HOMEOMORPHISMS

A Dissertation

Presented to the Faculty of the Graduate School
of Cornell University

in Partial Fulfillment of the Requirements for the Degree of
Doctor of Philosophy

by

Francesco Matucci

August 2008

© 2008 Francesco Matucci
ALL RIGHTS RESERVED

ALGORITHMS AND CLASSIFICATION IN GROUPS OF PIECEWISE-LINEAR HOMEOMORPHISMS

Francesco Matucci, Ph.D.

Cornell University 2008

The first part (Chapters 2 through 5) studies decision problems in Thompson's groups F, T, V and some generalizations. The *simultaneous conjugacy problem* is determined to be solvable for Thompson's group F and suitable larger groups of piecewise-linear homeomorphisms of the unit interval. We describe a conjugacy invariant both from the piecewise-linear point of view and a combinatorial one using *strand diagrams*. We determine algorithms to compute roots and centralizers in these groups and to detect periodic points and their behavior by looking at the *closed strand diagram* associated to an element. We conclude with a complete cryptanalysis of an encryption protocol based on the *decomposition problem*.

In the second part (Chapters 6 and 7), we describe the structure of subgroups of the group of all homeomorphisms of the unit circle, with the additional requirement that they contain no non-abelian free subgroup. It is shown that in this setting the *rotation number map* is a group homomorphism. We give a classification of such subgroups as subgroups of certain wreath products and we show that such subgroups can exist by building examples. Similar techniques are then used to compute centralizers in these groups and to provide the base to generalize the techniques of the first part and to solve the simultaneous conjugacy problem.

BIOGRAPHICAL SKETCH

Francesco Matucci was born on May 5th, 1977 in Florence, Italy to Annamaria Savi and Patrizio Matucci. He attended Liceo Guido Castelnuovo in Florence and went on to earn a *Laurea* in Mathematics *cum Laude* in April 2002 at the University of Florence. In December 2005 he earned a *Dottorato di Ricerca* at the University of Florence while studying abroad at Cornell University in Ithaca, NY, USA. He was admitted to the Mathematics graduate program at Cornell University in January 2006 and completed his Ph.D. studies in August 2008 under the supervision of Dr. Kenneth S. Brown and Dr. Martin D. Kassabov.

To whoever offered me a smile.

ACKNOWLEDGEMENTS

I would like to thank my two advisors Ken Brown and Martin Kassabov for their guidance, their time and many laughs. They have supported me through adverse times and shown me much deep mathematical thinking. I want to thank Ken who welcomed me into the graduate program as a father and lifted the many burdens of these years. I want to thank Martin, who has been a great friend and has always been available for help. It has been both a pleasure and an honor to work with them. I also want to thank the other members of my committee, Karen Vogtmann and R. Keith Dennis, for giving me important advice while deciding my future directions.

I want to thank all of the faculty and staff of the Cornell Department of Mathematics, but especially Maria Terrell for showing me the beauty of teaching and encouraging me to develop this passion. An important mention goes also to Donna Smith who has been the “glue” throughout these years, providing tremendous support in so many ways.

I would like to thank Indira Chatterji and Collin Bleak who have taken care of me remotely and shared their own experiences with me. I would also like to thank Matt Brin and José Burillo for giving me support throughout the enduring process of job searching.

I would like to thank Carlo Casolo who introduced me to the world of Mathematics as an undergraduate and who followed me even when I crossed the ocean.

Many friends also supported me in this process: my fellow graduate students who welcomed me and made me feel at home, in particular, thanks go to Brad, Jim, Jessica, Treven and Will. I want to thank Chris, Franco and Showey for just being my friends, entertaining me and showing me a new world. And

from the old country I would like to thank Luca and Massimo for reaching out at all times.

Finally I want to thank Hiromi for listening, looking after me and chasing me through the world. My parents come last in this list, but they know well they are first, because they are the ones who have taught me to smile.

TABLE OF CONTENTS

Biographical Sketch	iii
Dedication	iv
Acknowledgements	v
Table of Contents	vii
List of Tables	ix
List of Figures	x
Introduction	1
1 Thompson's groups F, T and V	8
1.1 Background on F	8
1.2 The generalized groups $PL_{S,G}(J)$ and the group $PL_+(J)$	13
1.3 Thompson's group T and V	14
2 Conjugacy in Thompson's groups	17
2.1 Conjugacy in Thompson's group F	18
2.2 Conjugacy in Thompson's group T	36
2.3 Conjugacy in Thompson's group V	45
2.4 Running Time	58
3 Dynamics in Thompson's Group F	62
3.1 Strand Diagrams	62
3.2 Dynamics of Annular Strand Diagrams	67
3.3 Mather Invariants	79
4 The Simultaneous Conjugacy Problem in Groups of Piecewise Linear Functions	90
4.1 The Ordinary Conjugacy Problem for $PL_2(I)$	91
4.2 Roots and Centralizers in $PL_2(I)$	118
4.3 The k -Simultaneous Conjugacy Problem in $PL_2(I)$	122
4.4 Stair Algorithm in $PL_{S,G}(I)$	130
4.5 Simultaneous Conjugacy Problem in $PL_{S,G}(I)$	144
4.6 Interesting Examples	146
5 Cryptanalysis of the Shpilrain-Ushakov protocol for Thompson's group	149
5.1 Introduction	149
5.2 The Protocol	151
5.3 The Subgroups A_s, B_s	152
5.4 Suggested Parameters for the Encryption	155
5.5 Recovering the Shared Secret Key	155
5.6 Transitivity of A_s and B_s	158
5.7 Using Transitivity to Attack the Shared Secret Key	161

5.8	Comments and Alternatives to the Protocol	163
6	Structure Theorems for Subgroups of Homeomorphisms Groups	167
6.1	Background and Tools	168
6.2	The Rotation Number Map is a Homomorphism	171
6.3	Applications: Margulis' Theorem	182
6.4	Structure and Embedding Theorems	184
6.5	Fixed-Point Free Actions on the Circle	193
7	Centralizers of subgroups of $\text{Homeo}_+(S^1)$	195
7.1	Centralizers of torsion elements	195
7.2	Non-torsion elements with rational <i>rot</i> number	200
7.3	More results on Centralizers	202
8	A Growth Formula for Thompson's Group F	205
8.1	Forest Diagrams	206
8.2	The Length Formula	210
8.3	Partitioning the n -sphere	212
8.4	A recurrence formula for the slices in 5 variables	215
8.5	Reducing the recurrence to 3 variables	221
8.6	Open Question: the Growth Series of F	223
A	Omitted Proofs	224
A.1	Chapter 2 Appendix: Positive Cochains	224
A.2	Chapter 4 Appendix: Some Computations	226
	Bibliography	229

LIST OF TABLES

8.1	The table of weight of the spaces	211
8.2	How λ reduces the length of elements	217

LIST OF FIGURES

1.1	The binary tree of dyadic intervals	9
1.2	An example of a dyadic subdivision	9
1.3	The tree corresponding to the subdivision in figure 1.2.	9
1.4	An example of a tree diagram	10
1.5	The reduction of a tree diagram	10
1.6	Two of the elements of the generating set of F	12
1.7	An element of F as a dyadic rearrangement of the unit interval. .	14
1.8	A dyadic rearrangement of the unit circle.	15
1.9	A tree diagram for the element of T	15
1.10	An element of V seen as a dyadic rearrangement.	16
1.11	A tree diagram for the element of V in figure 1.10.	16
2.1	A $(1, 1)$ -strand diagram	18
2.2	A split and a merge	19
2.3	Reductions	19
2.4	Diamond Lemma	20
2.5	An (m, n) -strand diagram	24
2.6	The right vine	25
2.7	An annular strand diagram	26
2.8	An example of a free loop in an annular strand diagram	27
2.9	Orientation of the cutting path	27
2.10	Reductions of an annular strand diagram	29
2.11	Diamond lemma in the annular case	30
2.12	Creating a conjugator	31
2.13	Moving the cutting path past the reduction area	32
2.14	A reduced annular strand diagram	33
2.15	Constructing an annular strand diagram	35
2.16	A cylindrical strand diagram	36
2.17	Reductions for a cylindrical strand diagram	37
2.18	A cylindrical strand diagram that is not reducible	37
2.19	From a tree diagram to a cylindrical strand diagram	37
2.20	From a cylindrical strand diagram to a tree diagram	38
2.21	An (m, n) -strand diagram	38
2.22	Toral strand diagrams that are not isotopic	40
2.23	Orientation of the cutting class	41
2.24	Reductions for a toral strand diagram	41
2.25	The torsion element c_n	45
2.26	An abstract strand diagram	46
2.27	Reductions for abstract strand diagrams	47
2.28	Non valid reduction.	47
2.29	From a tree diagram to an abstract strand diagram	47
2.30	A closed strand drawn on the punctured plane	49

2.31	Orientation of the cutting class	49
2.32	Reductions for closed strand diagrams	50
2.33	Cutting classes and reductions	51
2.34	Diamond Lemma	52
2.35	Same reduced closed strand diagram	52
2.36	Ribbon splits and merges	55
2.37	Ribbon reductions	56
2.38	An element of Thompson's group BV	57
2.39	Decorating the annular strand diagram.	59
3.1	A strand diagram as a circuit	63
3.2	Split rule	63
3.3	Merge rule	64
3.4	Reductions do not change the underlying map	65
3.5	An element of Thompson's groupoid	66
3.6	An example of an element of F	67
3.7	Completing an element out of a "pipeline"	71
3.8	Three conjugate elements	72
3.9	A minimal representative	73
3.10	The corresponding reduced annular strand diagram	73
3.11	An example of a merge loop	75
3.12	Traveling through the merge loop	76
3.13	An example of a split loop	76
3.14	Components of a function	78
3.15	Annular strand diagram for a component	78
3.16	A one-bump function	80
3.17	Action of f in a neighborhood of 0	81
3.18	The PLog map	84
3.19	Construction of the circle C_0	84
3.20	Annular strand diagram for a one-bump function	86
3.21	From an annular strand diagram to a cylindrical one	86
3.22	Labeling of a cylindrical strand diagram	87
3.23	A circle map	87
3.24	A forest diagram for the circle map	87
3.25	The constructed labeled cylindrical strand diagram	88
3.26	Traveling through a split loop	89
4.1	A function with a non-dyadic fixed point.	93
4.2	An example with $\partial D(y) \neq \partial D(z)$	94
4.3	How to build a $g \in \text{PL}_2(I)$, with $g(\alpha) = \beta$	96
4.4	y and z coincide around the endpoints.	99
4.5	Initial linearity box.	100
4.6	The identification trick	105
4.7	Mather invariant as an unlabeled cylindrical strand diagram	111

4.8	Cylindrical strand diagrams “differ” by a rotation on the top or on the bottom	112
4.9	The structure of centralizers in F	119
5.1	An example of an element of A_s and one of B_s	154
5.2	The two standard generators for $PL_2([0, \varphi_2])$	160
6.1	Two lifts of a circle homeomorphism.	168
6.2	A homeomorphism with rotation number $\frac{1}{4}$	169
6.3	A graphical description of the ping pong lemma.	171
6.4	The rotation map is not a homomorphism in general.	172
6.5	Two elements generating a free subgroup.	173
6.6	Intersecting bumps.	174
6.7	Non-intersecting bumps.	177
6.8	Making room for straight lines between \widehat{f} and \widehat{g}	180
6.9	How to build the map X_3 from X_2	192
8.1	A forest diagram for an element of F	206
8.2	Different trees	207
8.3	Reductions in a forest diagram.	207
8.4	The trivial forest diagram.	208
8.5	Some sample edges from the Cayley graph of F	209
8.6	The length of this element is 22	211
8.7	The trees T_+, T_- and the line $E = E(f)$	213
8.8	In this case $u(f) = 0$ and $w(f) = 5$	213
8.9	Here $b(f_1) = 4, c(f_1) = 1, b(f_2) = 1, c(f_2) = 0$	214
8.10	The action of λ when the top pointer is on T_+	216
8.11	The various possibilities for (\mathbf{Y}, \mathbf{X}) and (\mathbf{V}, \mathbf{X})	217
8.12	In each case $\ell(\lambda(f)) \leq \ell(f) - 1$	217
8.13	The map θ_1	218
8.14	The map θ_2	219
8.15	$\text{supp}(f) = \text{supp}(\lambda(f))$	220
8.16	$\text{supp}(\lambda(f))$ may be reduced.	221
A.1	The Farkas Lemma	225
A.2	The basic function to get transitivity.	226

INTRODUCTION

Decision Problems in Thompson's groups

My research started from studying decision problems for the important Thompson's groups F , T and V . These groups are piecewise-linear homeomorphism groups of a 1-dimensional space and were introduced in 1965 by R. Thompson in connection with his work in logic. They were introduced during the creation of a finitely generated group with unsolvable word problem, and later rediscovered in many other contexts. Thompson's groups provided the first known examples of finitely presented infinite simple groups and they are still at the center of many geometric group theory questions. What makes Thompson's groups an interesting starting point is that they are considered a test case for many conjectures. Even though the groups have a simple definition, many questions prove to be a challenge. Thompson's groups have many models: they can be described using generators and relations, or by their action on a 1-dimensional space or by representing elements as combinatorial diagrams. This characteristic often allows hard questions in one language to be transformed into easy questions in another one. They are often used as instruments to measure the understanding of a certain property. For example, it is an outstanding open question whether or not F is an amenable group.

Richard Thompson's group F can be seen as the group $PL_2([0, 1])$ of piecewise linear orientation-preserving homeomorphisms of the unit interval $[0, 1]$, with finitely many breakpoints such that:

- all slopes are integral powers of 2, and

- all breakpoints are in $\mathbb{Z}[\frac{1}{2}]$, the ring of dyadic rational numbers.

The product of two elements is given by the composition of functions. The group F is finitely presented (with two generators and two relations) and torsion-free.

In addition to F , Thompson introduced two other finitely-generated groups known as T and V . Briefly, T is the set of piecewise-linear self-homeomorphisms of the circle $[0, 1] / \{0, 1\}$ satisfying the two conditions above, while V is the set of piecewise-linear *bijections* of the interval (or self-homeomorphisms of the Cantor set) satisfying the above conditions. We will recall all relevant definitions and properties of Thompson's groups in Chapter 1.

We say that a group G has *solvable conjugacy problem* if there is an algorithm such that, given any two elements $x, y \in G$, we can determine whether there is, or not, a $g \in G$ such that $g^{-1}xg = y$. The conjugacy problem for F was addressed by Guba and Sapir [38], who solved it for general diagram groups in 1997, observing that F itself is a diagram group. In Chapter 2, we give a version of Guba and Sapir's solution using *strand diagrams*, and generalize it to T and V . To the best of our knowledge, the solution for T is entirely new. The material of Chapter 2 represents joint work with James Belk.

In Chapter 3 we derive an explicit correspondence between strand diagrams and piecewise-linear functions. Specifically, we show that strand diagrams can be interpreted as *stack machines* acting on binary expansions. Using this correspondence, we obtain a complete understanding of the dynamics of elements, describing the behavior of fixed points and their slopes. As a byproduct of our techniques, we obtain simple proofs of previously known results. In ad-

dition, we describe a completely dynamical solution to the conjugacy problem for one-bump functions in F , similar to the Brin-Squier [19] dynamical criterion for conjugacy in $PL_+(I)$, the group of all piecewise-linear orientation-preserving homeomorphisms of the unit interval with finitely many breakpoints. The material of Chapter 3 represents joint work with James Belk.

For a fixed $k \in \mathbb{N}$, we say that the group G has *solvable k -simultaneous conjugacy problem* if there is an algorithm such that, given any two k -tuples of elements in G , $(x_1, \dots, x_k), (y_1, \dots, y_k)$, one can determine whether there is, or not, a $g \in G$ such that $g^{-1}x_i g = y_i$ for all $i = 1, \dots, k$. We say that there is an *effective solution* if the algorithm produces such an element g , in addition to proving its existence. In 1999, Guba and Sapir [37] posed the question of whether or not the simultaneous conjugacy problem was solvable for diagram groups. In Chapter 4 we prove

Theorem A. *Thompson's group F has a solvable k -simultaneous conjugacy problem, for every $k \in \mathbb{N}$. There is an algorithm which produces an effective solution.*

With similar techniques we can prove that the same result holds for larger groups of piecewise linear homeomorphisms, containing F as a subgroup. The material of Chapter 4 represents joint work with Martin Kassabov.

Decision Problems and Cryptography

Recent advances in public key cryptography have underlined the need to find alternatives to the RSA cryptosystem. It has been proposed to use algorithm-

mic problems in non-commutative group theory as possible ways to build new protocols. The *conjugacy search problem* was introduced in several papers as a generalization of the *discrete logarithm problem* in the research of a new safe encryption scheme. The former problem asks whether or not, given a group G and two elements $a, b \in G$ that are conjugate, we can find at least one $x \in G$ with $a^x := x^{-1}ax = b$. It is thus important to look for a platform group G where this problem is computationally hard. Seminal works by Anshel-Anshel-Godlfeld [2] and Ko-Lee et al. [44] have proposed the braid group B_n on n strands as a possible platform group.

It has been observed that Thompson's group F and the braid groups B_n have some similarities. Belk proved in his thesis [5] that F and the braid groups have a similar classifying space. Strand diagrams for elements of F (introduced in Chapter 2) are similar to braids, but with merges and splits instead of twists. However, for cryptographic purposes, F has still not proved to be a good platform. Theorem A proves that the simultaneous conjugacy problem is solvable, making it insecure to apply protocols based on the simultaneous conjugacy problem.

Shpilrain and Ushakov in [61] have proposed using a particular version of the *decomposition problem* as a protocol and the group F as a platform. The new problem is: given a group G , a subset $X \subseteq G$ and two elements $w_1, w_2 \in G$ with the information that there exist $a, b \in X$ such that $aw_1b = w_2$, find at least one such pair a, b . In Chapter 5 we show how to recover efficiently the shared secret key of this protocol.

Structure Theorems for $\text{Homeo}_+(S^1)$ and Centralizers

Let $\text{Homeo}_+(S^1)$ denote the full group of orientation-preserving homeomorphisms of the unit circle and G be one of its subgroups. Many papers have studied the structure of subgroups under particular assumptions. Plante and Thurston have discovered that sufficient smoothness imposes a strong condition on nilpotent groups of orientation-preserving diffeomorphisms.

Theorem (Plante-Thurston, [51]). *Any nilpotent subgroup of $\text{Diff}_+^2(S^1)$ must be abelian.*

On the other hand, Farb and Franks showed that reducing the smoothness produces a contrasting situation, where every possibility can occur.

Theorem (Farb-Franks, [28]). *Every finitely-generated, torsion-free nilpotent group is isomorphic to a subgroup of $\text{Diff}_+^1(S^1)$.*

In Chapter 6 we relax the hypotheses on the regularity of the homeomorphisms and on the group. We explore the dynamics of Poincaré's rotation number map $\text{rot} : G \rightarrow \mathbb{R}/\mathbb{Z}$: under certain conditions, it is possible to prove that the rot map becomes a homomorphism of groups. In particular, we obtain a result in the flavor of the Tits Alternative:

Theorem B. *Let $G \leq \text{Homeo}_+(S^1)$. Then the following alternative holds:*

- (i) *G has a non-abelian free subgroup, or*
- (ii) *the map $\text{rot} : G \rightarrow (\mathbb{R}/\mathbb{Z}, +)$ is a group homomorphism.*

Part (ii) of this first result allows us to write subgroups of $\text{Homeo}_+(S^1)$ as ex-

tensions of the kernel by a subgroup of \mathbb{R}/\mathbb{Z} and hence to reduce the classification to studying the kernel of the *rot* map. As a byproduct, we obtain Margulis' Theorem on the existence of a G -invariant measure on the unit circle (see [47]).

Theorem C. *Let $G \leq \text{Homeo}_+(S^1)$ with no non-abelian free subgroups. Then:*

(i) *G is abelian, or*

(ii) *$G \hookrightarrow H_0 \wr K$, the standard unrestricted wreath product, where $K := G/G_0$ is isomorphic to a countable subgroup of \mathbb{R}/\mathbb{Z} and $H_0 \leq \prod \text{Homeo}_+(I_i)$ has no non-abelian free subgroups.*

We will show that such wreath products do exist in $\text{Homeo}_+(S^1)$ by providing embedding theorems. The material of Chapter 6 represents joint work with Collin Bleak and Martin Kassabov.

The techniques developed in Chapter 6 are then employed in Chapter 7 to obtain some results on centralizers of elements and subgroups in $\text{PL}_+(S^1)$ the group of orientation-preserving piecewise-linear homeomorphisms of the unit circle with finitely many breakpoints. Centralizers are used in Chapter 4 as an intermediate step to go from the solution of the ordinary conjugacy problem to the solution of the simultaneous conjugacy one. It is thus of interest to classify centralizers in groups of homeomorphisms of the unit circle to generalize our results to this setting. The material of Chapter 7 represents joint work with Collin Bleak and Martin Kassabov.

Estimating the size of balls in Thompson's group F

In the last Chapter we describe a recurrence formula relating suitable slices of the n -sphere of Thompson's group F with those of spheres of smaller radius, where elements are written with respect to the standard finite generating set of F . The algorithm is based on the length formula for elements developed in [4] by Belk and Brown. We study their formula to detect what is the correct pattern to shorten a word to the identity element. To the best of our knowledge, no other formula existed before to estimate the size of balls (besides direct counting of elements).

CHAPTER 1

THOMPSON'S GROUPS F, T AND V

In this Chapter we recall the main definitions and results about Thompson's groups F, T and V and some of their overgroups. The proofs of all the stated results of this Chapter can be found either in [25] or in [5], unless otherwise stated.

1.1 Background on F

Let I denote the unit interval $[0, 1]$. Thompson's group F is the group of all piecewise-linear homeomorphisms of the unit interval with finitely many breakpoints and satisfying the following conditions:

1. Every slope is a power of two, and
2. Every breakpoint has dyadic rational coordinates.

The group F is finitely presented (with two generators and two relations) and torsion-free. It can be thought of as a "lattice" in the full group $\text{PL}_+(I)$ of orientation-preserving piecewise-linear homeomorphisms of $[0, 1]$ with finitely many breakpoints, and indeed it shares many properties with this larger group.

We are now going to describe how to see the elements of F as diagrams. Consider the subintervals of I obtained by repeatedly cutting in half (see figure 1.1).

These are the *standard dyadic intervals*. A dyadic subdivision of I is any partition into finitely many standard dyadic intervals (see figure 1.2).

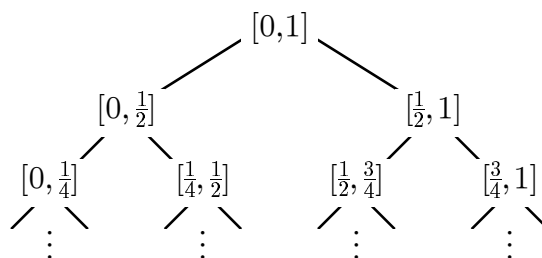


Figure 1.1: The binary tree of dyadic intervals

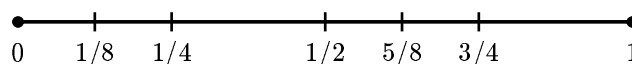


Figure 1.2: An example of a dyadic subdivision

Dyadic subdivisions correspond to finite subtrees of the infinite binary tree (the dyadic subdivision of figure 1.1 becomes the tree represented in figure 1.3). A *dyadic rearrangement* is a homeomorphism $f : I \rightarrow I$ that maps intervals of one dyadic subdivision linearly to the intervals of another.

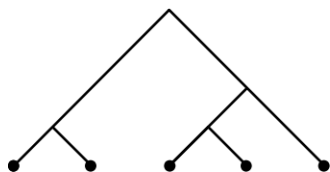


Figure 1.3: The tree corresponding to the subdivision in figure 1.2.

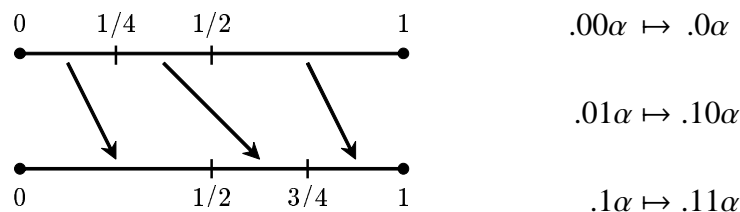


Figure 1.3.1: a dyadic rearrangement

If we represent elements of $[0, 1]$ in binary, a dyadic rearrangement acts as a prefix replacement rule on binary sequences, as illustrated in figure 1.3.1.

Proposition 1.1.1. *The elements of Thompson’s group F are precisely the dyadic rearrangements of I .*

A *Tree diagram* for an element $f \in F$ is a pair of rooted, binary trees that describe the dyadic subdivisions of the domain and range (see figure 1.4).

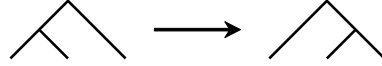


Figure 1.4: An example of a tree diagram

The tree diagram for an element of F is not entirely unique. Specifically, we can reduce a tree diagram by canceling a corresponding pair of bottom caret (see figure 1.5).

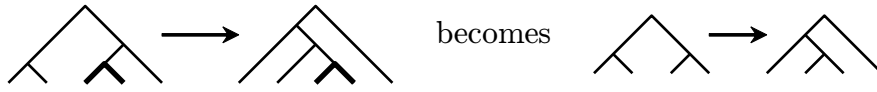


Figure 1.5: The reduction of a tree diagram

This corresponds to removing an unnecessary “cut” from the domain and range subdivisions. We say that two tree diagrams are equivalent if one can obtained from the other via a sequence of reductions and inverse reductions.

Theorem 1.1.2. *Every element of F has a unique reduced tree diagram. Moreover, the elements of Thompson’s group F are in 1-to-1 correspondence with reduced tree diagrams.*

It is possible to define a product in the set of equivalence classes of tree diagrams corresponding to the product in F . Given two representatives for equivalence classes of tree diagrams $f : T_1 \rightarrow T_2$ and $g : T_3 \rightarrow T_4$, it is possible to unreduce them until the range tree of f is the same as the domain tree for g , that

is we can write $f : T'_1 \rightarrow T'_2$ and $g : T'_2 \rightarrow T'_4$ and then the product fg is defined as the equivalence class of the tree diagram $fg : T'_1 \rightarrow T'_4$. This product agrees with the product of piecewise-linear homeomorphisms, hence Thompson's group F is isomorphic with the group of equivalence classes of tree diagrams.

As we stated above Thompson's group admits a finite presentation, however we will not need it. Instead, in Chapter 5 we will make use of the infinite presentation described in the next result.

Theorem 1.1.3. *Thompson's group F is described by the following presentation*

$$F = \langle x_0, x_1, x_2, \dots \mid x_n x_k = x_k x_{n+1}, \forall k < n \rangle.$$

This presentation has the advantage that the elements of F can be uniquely written in the following *normal form*

$$x_{i_1} \dots x_{i_u} x_{j_v}^{-1} \dots x_{j_1}^{-1}$$

such that $i_1 \leq \dots \leq i_u$, $j_1 \leq \dots \leq j_v$ and if both x_i and x_i^{-1} occur, then either x_{i+1} or x_{i+1}^{-1} occurs, too. Since $x_k = x_0^{1-k} x_1 x_0^{k-1}$ for $k \geq 2$, the group F is generated by the elements x_0 and x_1 . The generators x_k of the infinite presentation can be represented as piecewise-linear homeomorphisms by shrinking the function x_0 shown in figure 1.6 onto the interval $[1 - \frac{1}{2^k}, 1]$ and extending it as the identity on $[0, 1 - \frac{1}{2^k}]$.

Lemma 1.1.4. *If $0 = a_0 < a_1 < a_2 < \dots < a_n = 1$ and $0 = b_0 < b_1 < b_2 < \dots < b_n = 1$ are two partitions of $[0, 1]$ consisting of dyadic rational numbers, then we can build an $f \in F$, such that $f(a_i) = b_i$. In particular, F acts transitively on k -tuples of dyadic points in $(0, 1)$ for any k .*

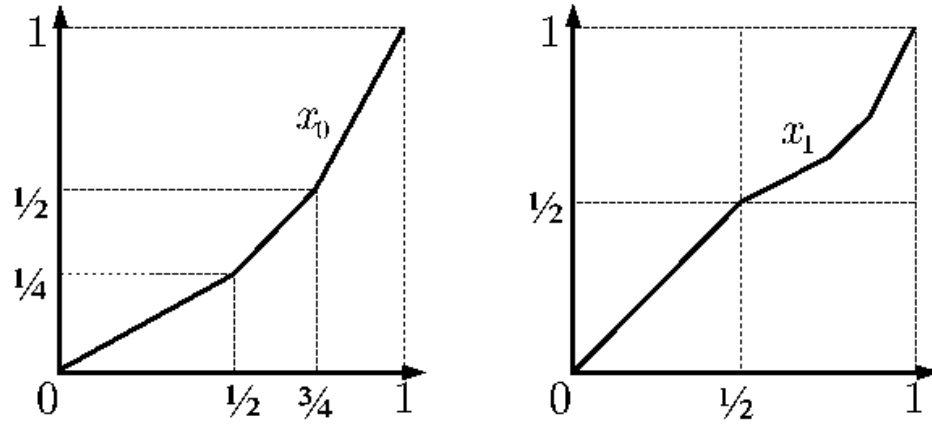


Figure 1.6: Two of the elements of the generating set of F .

For an interval $J \subseteq \mathbb{R}$ with dyadic endpoints, it is possible to define Thompson-like analogues of Thompson's group F . We can consider the groups $\text{PL}_2(J)$ of piecewise-linear homeomorphism on the interval J onto itself with finitely many breakpoints and the same requirements on slopes and breakpoints as F .

Theorem 1.1.5. *For any two dyadic rationals $\alpha < \beta$ in the real line \mathbb{R} , there exists a Thompson-like homeomorphism $\varphi : [\alpha, \beta] \rightarrow [0, 1]$, i.e. a piecewise-linear homeomorphisms with finitely many breakpoints occurring at dyadic rationals and whose slopes are integral powers of 2.*

Proof. This is a well known fact, but we provide a proof for the sake of completeness. Let $m < n$ be a pair of integers such that $[0, 1] \cup [\alpha, \beta] \subseteq (m, n)$ and such that $m - n = 2^v$, for some integer v . If we consider the straight line map $\psi : [m, n] \rightarrow [0, 1]$, it is straightforward to verify that the choice of m, n implies that the map $\rho(G) := \psi G \psi^{-1}$ yields an isomorphism $\rho : \text{PL}_2([m, n]) \rightarrow \text{PL}_2(I)$. To construct the required Thompson-like map it is sufficient to consider $m < \alpha < \beta < n$ and $m < 0 < 1 < n$ as partitions of the interval $[m, n]$ and bring them to the

interval $[0, 1]$ through ψ . Hence, we can apply Lemma 1.1.4 to find an element $f \in \text{PL}_2(I)$ that sends the partition $0 = \psi(m) < \psi(\alpha) < \psi(\beta) < \psi(n) = 1$ into the partition $0 < \psi(0) < \psi(1) < 1$ to find an element $f \in \text{PL}_2(I)$. To conclude, it is sufficient to define φ as the restriction of $\rho^{-1}(f)$ to the interval $[\alpha, \beta]$. \square

Corollary 1.1.6. *For any two dyadic rationals $\alpha < \beta$ in the interval $[0, 1]$, the groups $\text{PL}_2([\alpha, \beta])$ and $\text{PL}_2(I)$ are isomorphic.*

Proof. By Theorem 1.1.5, there is a Thompson-like map $\varphi : [\alpha, \beta] \rightarrow [0, 1]$. Now define

$$\begin{aligned} \text{PL}_2([\alpha, \beta]) &\longrightarrow \text{PL}_2(I) \\ f &\longmapsto \varphi f \varphi^{-1} \quad \square \end{aligned}$$

The previous two results are used at many points in this thesis: for example we will use them in Chapters 3, 4 and 7.

1.2 The generalized groups $\text{PL}_{S,G}(J)$ and the group $\text{PL}_+(J)$

In Chapter 4 we will work with a generalization of Thompson's group F by relaxing the hypotheses on breakpoints and slopes. Let S be a subring of \mathbb{R} , let $U(S)$ denote the group of invertible elements of S and let G be a subgroup of $U(S) \cap \mathbb{R}_+$. For any interval J with endpoints in S , we define $\text{PL}_{S,G}(J)$ to be the group of piecewise linear homeomorphism from the interval J into itself, with only a finite number of breakpoints and such that

- all breakpoints are in the subring S ,
- all slopes are in the subgroup G ,

the product of two elements being given by the composition of functions. Unlike the case of F and Corollary 1.1.6, it is not true anymore that for any two intervals J_1, J_2 with endpoints in S the groups $\text{PL}_{S,G}(J_1)$ and $\text{PL}_{S,G}(J_2)$ are isomorphic. For any interval J , we denote by $\text{PL}_+(J)$ the group of piecewise-linear orientation-preserving homeomorphisms of the interval J , with finitely many breakpoints. Since there are no requirements for the breakpoints and the slopes of elements of $\text{PL}_+(J)$ then, for any subring S and $G \leq U(S) \cap \mathbb{R}_+$, we have $\text{PL}_{S,G}(J) \subseteq \text{PL}_+(J)$.

1.3 Thompson's group T and V

Thompson's group F is the group of dyadic rearrangements on the unit interval. The important requirement is that these rearrangements preserve the order of the intervals of the partition (see figure 1.7).

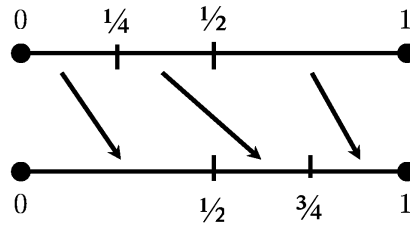


Figure 1.7: An element of F as a dyadic rearrangement of the unit interval.

We can relax the last requirement on the order of intervals and require that these rearrangements preserve the cyclic order of intervals (see figure 1.8). Thompson's group T is the group of dyadic rearrangements of $[0, 1]$ that preserve the cyclic order. Since the elements of T preserve the cyclic order of subdivisions of $[0, 1]$ they can be viewed as homeomorphisms of the unit circle.

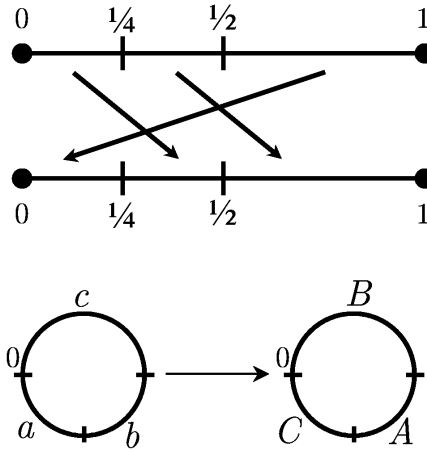


Figure 1.8: A dyadic rearrangement of the unit circle.

It is possible to define tree diagrams for elements of T . They correspond to dyadic rearrangements of the unit circle and are thus represented by a pair of rooted, binary trees along with a cyclic permutation of the leaves (see figure 1.9).

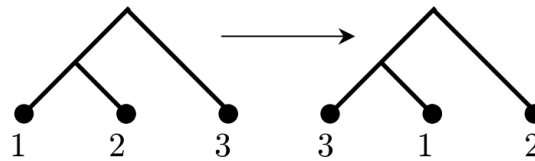


Figure 1.9: A tree diagram for the element of T .

If we allow a dyadic rearrangement to permute the order of intervals arbitrarily, we obtain a larger group containing F and T . *Thompson's Group V* is the group of dyadic rearrangements of $[0, 1]$ that may permute the order of the subdivisions (see figure 1.10).

Note that this produces bijections $[0, 1] \rightarrow [0, 1]$ that are *not* continuous. (By convention, all functions in V are required to be continuous from the right. Alternatively, one can define V as a group of homeomorphisms of the Cantor set.) The set of all elements of V forms a group under composition.

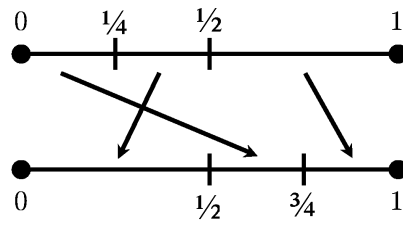


Figure 1.10: An element of V seen as a dyadic rearrangement.

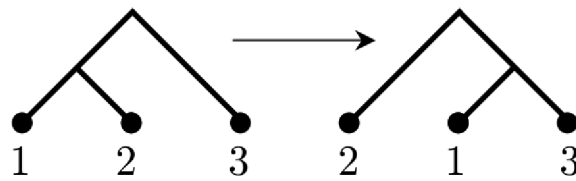


Figure 1.11: A tree diagram for the element of V in figure 1.10.

Even for V it is possible to define tree diagrams, which will appear as a pair of rooted, binary trees along with a permutation of the leaves (see figure 1.11).

CHAPTER 2

CONJUGACY IN THOMPSON'S GROUPS

In this Chapter we give a unified solution for the conjugacy problem in Thompson's groups F, T and V . We introduce *strand diagrams*, a modification of tree diagrams for these groups, and show how identifying the roots of the two trees defines a conjugacy invariant in all cases. This reduces the conjugacy problem to the study of the isomorphism problem for certain classes of graphs and gives us elementary proofs of some known results. Strand diagrams were first introduced by Pride in his study of the homotopy of relations using the term *pictures* in [52], [53] and [10] and are dual to the diagrams introduced by Guba and Sapir.

In 1997 Guba and Sapir showed that F can be viewed as a *diagram group* for the monoid presentation $\langle x \mid x^2 = x \rangle$ [38]. They give a solution for each diagram group, and in particular for F . Their solution amounted to an algorithm which had the same complexity as the isomorphism problem for planar graphs. This last problem has been solved in linear time in 1974 by Hopcroft and Wong [41], thus proving the Guba and Sapir solution of the conjugacy problem for diagram groups optimal. We mention here relevant related work: in 2001 Brin and Squier in [19] produced a criterion for describing conjugacy classes in $PL_+(I)$. In 2007 Gill and Short [32] extended this criterion to work in F , thus finding another way to characterize conjugacy classes from a piecewise linear point of view.

The conjugacy problem in V was previously solved by Higman [40] by combinatorial group theory methods and again by Salazar-Diaz [58] by using the techniques introduced by Brin in his paper [15]. On the other hand, to the best of our knowledge, the solution for T is entirely new.

This Chapter is organized as follows. In section 1 we give a simplified solution to the conjugacy problem in F . We extend this solution to T in section 2, and to V in section 3, and in section 4 we analyze the running time of the algorithm. Finally, we have relegated to the appendix a proof that every closed strand diagram for a conjugacy class in F , T , or V possesses a cutting path. The material of this Chapter represents joint work with James Belk. It can also be found in [6].

2.1 Conjugacy in Thompson's group F

2.1.1 Strand Diagrams

In this section, we describe Thompson's group F as a group of *strand diagrams*. A strand diagram is similar to a braid, except instead of twists, there are splits and merges (see figure 2.1).

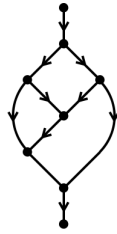


Figure 2.1: A $(1, 1)$ -strand diagram

To be precise, a *strand diagram* (or a $(1, 1)$ -strand diagram) is any directed, acyclic graph in the unit square satisfying the following conditions:

1. There exists a unique univalent source along the top of the square, and a unique univalent sink along the bottom of the square.

2. Every other vertex lies in the interior of the square, and is either a *split* or a *merge* (see figure 2.2).

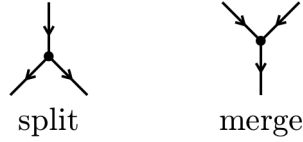


Figure 2.2: A split and a merge

As with braids, isotopic strand diagrams are considered equal. A *reduction* of a strand diagram is either of the moves shown in figure 2.3.

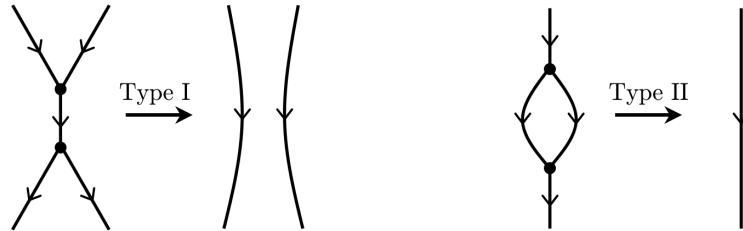


Figure 2.3: Reductions

Two strand diagrams are *equivalent* if one can be obtained from the other via a sequence of reductions and inverse reductions. A strand diagram is reduced if it is not subject to any reductions.

Proposition 2.1.1. *Every strand diagram is equivalent to a unique reduced strand diagram.*

Proof: This result was first proved by Kilibarda [43], and appears as lemma 3.16 in [38]. We repeat the proof here, for we must prove several variations of this result later. Consider the directed graph \mathcal{G} whose vertices are strand diagrams, and whose edges represent reductions. We shall use Newman's Diamond Lemma (see [50]) to show that each component of \mathcal{G} contains a unique terminal vertex.

Clearly \mathcal{G} is terminating, since each reduction decreases the number of vertices in a strand diagram. To show that \mathcal{G} is locally confluent, suppose that a strand diagram is subject to two different reductions, each of which affects a certain pair of vertices. If these two pairs are disjoint, then the two reductions simply commute. The only other possibility is that the two pairs have a vertex in common, in which case the two reductions have the same effect (figure 2.4).

□

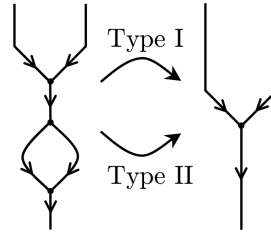


Figure 2.4: Diamond Lemma

The advantage of strand diagrams over tree diagrams is that *multiplication* is the same as concatenation (see figure 2.4.1).

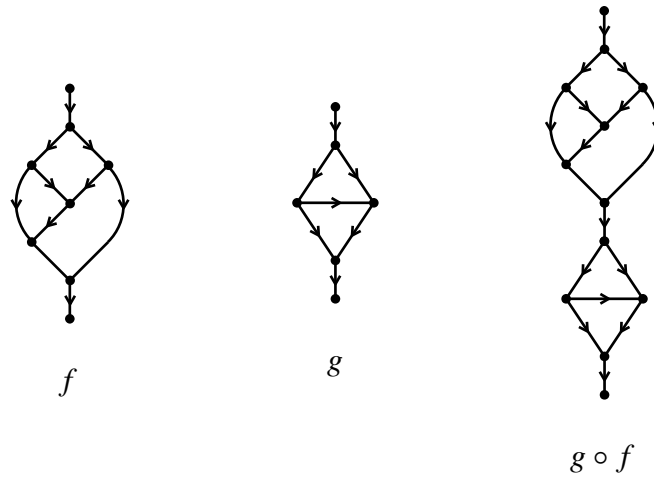


Figure 2.4.1: Product is given by concatenating diagrams

This algorithm is considerably simpler than the standard multiplication algorithm for tree diagrams (see Chapter 1). The *inverse* of a strand diagram is ob-

tained by reflection across a horizontal line and by inverting the direction of all the edges. Note that the product of a strand diagram with its inverse is always equivalent to the identity.

Theorem 2.1.2. *Thompson's group F is isomorphic with the group of all equivalence classes of strand diagrams, with product induced by concatenation.*

Proof. There is a close relationship between strand diagrams and the well-known tree pair diagrams for elements of F . In particular, a strand diagram for an element $f \in F$ can be constructed by gluing the two trees of a tree pair diagram together along corresponding leaves, after turning one tree upside down (see figure 2.4.2).

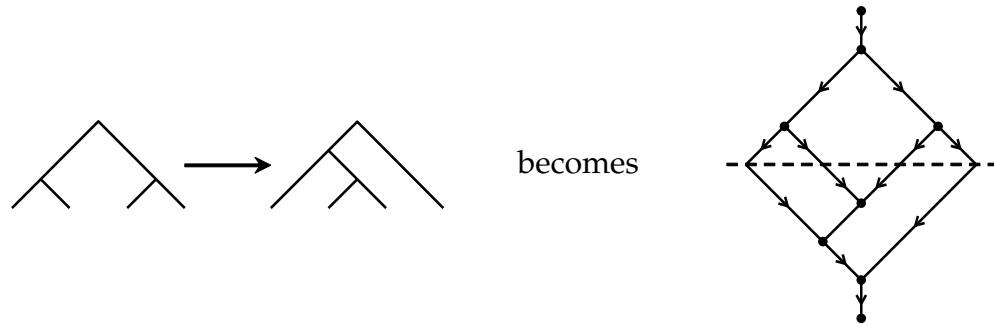


Figure 2.4.2: Gluing a tree diagram

Conversely, any reduced strand diagram can be “cut” in a unique way to obtain a reduced pair of binary trees (see figure 2.4.3).

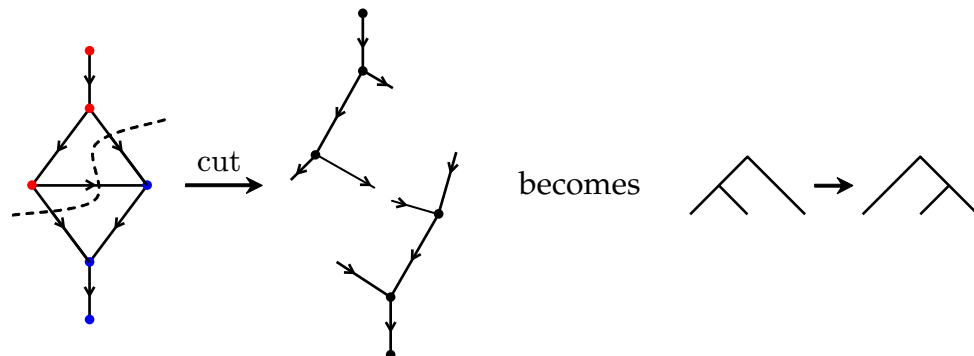


Figure 2.4.3: Cutting a strand diagram

We will now give a more formal proof of the intuition given by the previous two figures. We define the following three sets: $\mathcal{SD} = \{\text{reduced strand diagrams}\}$, $\mathcal{TD} = \{\text{reduced tree diagrams}\}$ and $PL_2(I)$ is the piecewise linear description of F . We want to prove that the previous three groups are isomorphic. Define the following map

$$\begin{aligned}\varphi: \mathcal{SD} &\longrightarrow PL_2(I) \\ D &\longmapsto f_D\end{aligned}$$

To build $f_D(t)$ we construct a path through the diagram which carries along a number that will change at each vertex. Given a number $t \in [0, 1]$ we write it in binary expansion $t = 0.b_1b_2\dots$. We start with t at the source and follow the outgoing edge. If we meet a split, we remove the first bit b_1 from t obtaining a new number $t' = 0.b_2\dots$. We then exit from the left if $b_1 = 0$ and from the right otherwise. We keep this going until we meet a merge. If we meet a merge with a number $0.a_1\dots$ we add a new first bit, obtaining a number $0.a_0a_1\dots$. The number a_0 that we add is a 0 if we arrived to the merge from the left and a 1 otherwise. We now iterate this pattern for all the splits and merges that we encounter, until we exit through the unique output of the strand diagram (the sink).

The number that remains at the end of this procedure is called $f_D(t)$. It is not difficult to see that each map $f_D(t)$ is a homeomorphism and that the map φ is a homomorphism (we will describe this construction in more detail in Chapter 3).

Given a reduced strand diagram D there is a way to cut it into two halves which are both directed trees. We consider the set of edges that leave all the

splits above and all the merges below and cut each of them. More precisely, to determine this set of edges, we use the following procedure: start with the set containing only the edge leaving the source, replace it with its two children. Now, if an edge terminates in a split, replace it with its two children. We repeat until we remain with a set of edges each of which terminates in a merge. It is not difficult to prove that this procedure is well defined, using the Diamond Lemma. Moreover, it is clear that what lies above these edges is a tree, and that what lies below must also be a tree (otherwise the diagram would not be reduced, or the set of edges is not minimal according to the previous procedure)

Thus, there exists at least one cut dividing a strand diagram into a tree diagram. A priori, there might be more than one way to cut the diagram in two trees, hence we need to prove that there is only one such cut. We build the following diagram

$$\begin{array}{ccc} \mathcal{SD} & \xrightarrow{\varphi} & PL_2(I) \\ & \swarrow \sigma & \uparrow \mu \\ & & \mathcal{TD} \end{array}$$

where σ is the map obtained by taking a tree diagram and gluing all its corresponding leaves to get a strand diagram and μ is the standard map which associates a piecewise-linear homeomorphism to a tree diagram (see Chapter 1). By definition of the maps, the diagram is commutative.

Let $D \in \mathcal{SD}$ and choose some cut v on the edges of D which divides D into two directed trees and define T_v to be the tree diagram associated to this cut.

Claim: The tree diagram T_v is independent of the choice of the cut v .

Proof of the Claim. Since the map σ glues back the points where we have cut D ,

we have that $\sigma(T_v) = D$. Hence we get

$$\mu(T_v) = \varphi\sigma(T_v) = \varphi(D).$$

By applying μ^{-1} to both sides of the previous equality, we get $T_v = \mu^{-1}\varphi(D)$ and therefore T_v is the image of a map and is then defined independently of the chosen cut. \square

The previous Claim allows us to well-define a map

$$\begin{aligned} \psi : \mathcal{SD} &\longrightarrow \mathcal{TD} \\ D &\longmapsto T_v \end{aligned}$$

By the proof of the Claim, we have shown that $\mu\psi = \varphi$. Moreover, the relations $\sigma\psi = id_{\mathcal{SD}}$ and $\psi\sigma = id_{\mathcal{TD}}$ follow easily. Therefore ψ is bijective, and it is clearly a homomorphism. \square

Note 2.1.3. We will sometimes need to consider more general strand diagrams, with more than one source and sink (see figure 2.5).

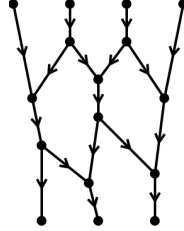


Figure 2.5: An (m, n) -strand diagram

We call an object like this an (m, n) -strand diagram, where m is the number of sources and n is the number of sinks. This graph is built with the same conditions as $(1, 1)$ -strand diagrams, except that it is allowed to have multiple sources and sinks. We observe that, for every positive integer k the equivalence classes of (k, k) -strand diagrams equipped with the product given by concatenation returns a group. It is possible to prove that the group of all $(1, 1)$ -strand diagrams

is isomorphic to the group of all (k, k) -strand diagrams, for every positive integer k . In fact, if we denote by v_m the right vine with m leaves (figure 2.6).

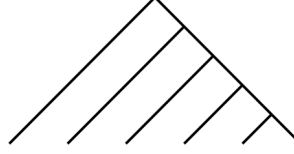


Figure 2.6: The right vine

then any (k, k) -strand diagram can be identified with the corresponding $(1, 1)$ -strand diagram given by $v_k^{-1} f v_k$ of Thompson's group F . In particular, we can compose two elements of F by concatenating any corresponding pair of strand diagrams. The previous description can be seen more formally from a categorical point of view. We consider a category C , where $Obj(C) = \mathbb{N}$, $Mor(C) = \{\text{morphisms } i \rightarrow j \text{ are labeled binary forests with } i \text{ trees and } j \text{ total leaves}\}$ (notice that the labeling on the trees induces a labeling on the leaves). The composition of two morphisms $f : i \rightarrow j$ and $g : j \rightarrow k$, is the morphism $fg : i \rightarrow k$ obtained by attaching the roots of the trees of g to the leaves of f by respecting the labeling on the roots of g and the leaves of f . With this definition, the equivalence classes of strand diagrams with any number of sources and sinks is the groupoid of fractions of the category C (more details on this construction can be found in [5]). We call this *Thompson's groupoid* \mathcal{F} . From the categorical point of view, we see that the projection $f \mapsto v_n^{-1} f v_m$ is an epimorphism from the groupoid \mathcal{F} to the group F .

2.1.2 Annular Strand Diagrams

Definition 2.1.4. An *annular strand diagram* is a directed graph embedded in the annulus with the following properties:

1. Every vertex is either a merge or a split.
2. Every directed cycle has positive winding number around the central hole.

Our definition of graph allows the existence of *free loops*, i.e. directed cycles with no vertices on them. Every element of F gives an annular strand diagram: given a strand diagram in the square, we can identify the top and bottom and delete the resulting vertex to get an annular strand diagram (figure 2.7).

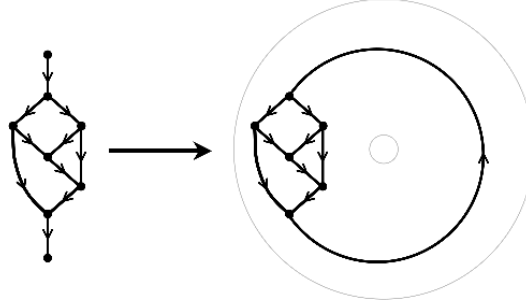


Figure 2.7: An annular strand diagram

More generally, you can obtain an annular strand diagram from any (k, k) -strand diagram in the square, for any $k \geq 1$. We observe that we may obtain free loops with no vertices (figure 2.8)

Definition 2.1.5. A *cutting path* for an annular strand diagram is a continuous path in the annulus that satisfies the following conditions:

1. The path begins on the inner circle of the annulus, and ends on the outer circle.

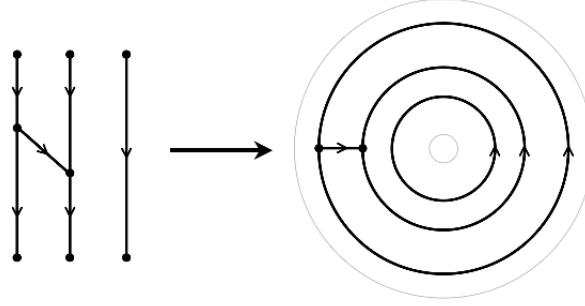


Figure 2.8: An example of a free loop in an annular strand diagram

2. The path does not pass through any vertices of the strand diagram.
3. The path intersects edges of the strand diagram transversely, with the orientation shown in figure 2.9.

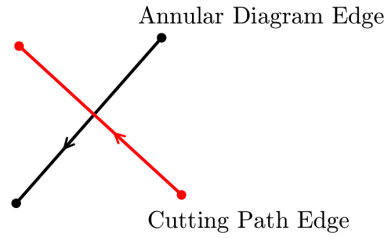


Figure 2.9: Orientation of the cutting path

Cutting an annular strand diagram along a cutting path yields a (k, k) -strand diagram embedded in the unit square (thus an element of Thompson's group F , by Note 2.1.3). Conversely, given an element of F as a (k, k) -strand diagram we can build an *associated annular strand diagram* by gluing the i -th source and the i -th sink, for $i = 1, \dots, k$. This gluing also defines a cutting path for the associated annular diagram. On the other hand, it can be shown that every annular strand diagram has at least one cutting path, hence any annular strand diagram is the associated annular strand diagram for some (k, k) -strand diagram. We sketch a proof of this fact, even though it will not be used in the characterization of conjugacy for elements of F seen as strand diagrams.

Theorem 2.1.6. *Every annular strand diagram has a cutting path.*

Sketch of a Proof: Let S be an annular strand diagram, and let c be the class in $H^1(S)$ induced by winding number on the annulus. By theorem A.1.1 in the appendix, there exists a cochain α on S representing c which takes a non-negative value on each directed edge.

If we regard the directed graph S as embedded in the plane, we observe that S divides the plane into regions and we can define S^* the directed dual graph to S . That is, S^* is the graph with one vertex for each region of S —including a vertex i for the inner region and a vertex o for the outer region—and with directed edges that transversely intersect the directed edges of S in the same manner as a cutting path. The cochain α on S can be viewed as a chain α^* on S^* , which is a positive linear combination of directed edges. In particular, the boundary of α^* must be the difference $o - i$. Then α^* must be the sum of directed cycles and a single directed path from i to o , the latter being the desired cutting path. \square

Definition 2.1.7. A reduction of an annular strand diagram is any of the three types of moves shown in figure 2.10.

In the third move, two concentric free loops with nothing in between are combined into one. Note that a reduction of an annular strand diagram yields an annular strand diagram. Note also that any two annular strand diagrams for the same element of F are equivalent.

Proposition 2.1.8. *Every annular strand diagram is equivalent to a unique reduced annular strand diagram.*

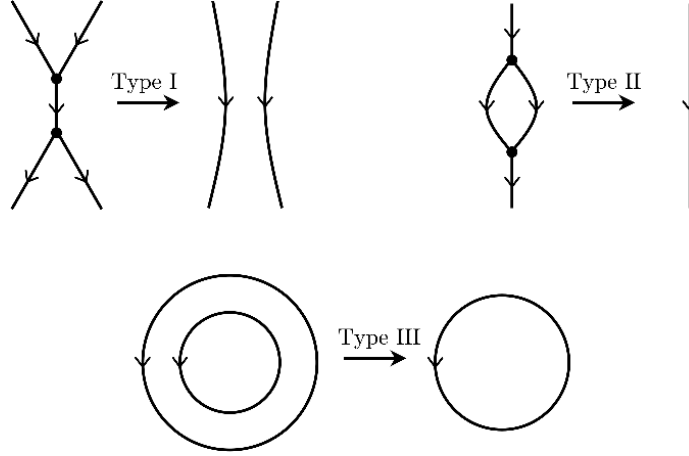


Figure 2.10: Reductions of an annular strand diagram

Proof: We shall use Newman's Diamond Lemma (see [50]). Clearly the process of reduction terminates, since any reduction reduces the number of edges. We must show that reduction is locally confluent.

Suppose that a single annular strand diagram is subject to two different reductions. If one of these reductions is of type III, then the two reductions commute: if the other one is of type I or II, then the reductions must act on disjoint connected components of the diagram, while if the other is of type III too, we can collapse all adjacent free loops in any given order. Otherwise, both of the reductions involve the removal of exactly two trivalent vertices. If the reductions remove disjoint sets of vertices, then they commute. If the reductions share a single vertex, then the results of the two reductions are the same (see figure 2.4). Finally, it is possible for the reductions to involve the same pair of vertices, in which case they can be resolved with a reduction of type III (see figure 2.11).

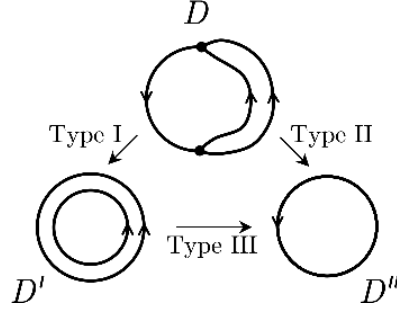


Figure 2.11: Diamond lemma in the annular case

2.1.3 Characterization of Conjugacy in F

The goal of this section is to prove the following theorem:

Theorem 2.1.9. *Two elements of F are conjugate if and only if they have the same reduced annular strand diagram.*

It is not hard to see that conjugate elements of F yield the same reduced annular strand diagram. The task is to prove that two elements of F with the same reduced annular strand diagram are conjugate.

We begin with the following proposition, whose proof closely follows the arguments of Guba and Sapir regarding conjugacy [38].

Proposition 2.1.10. *Any two cutting paths for the same annular strand diagram yield conjugate elements of F .*

Proof: Let σ_1 and σ_2 be cutting paths for the same annular strand diagram, and let g_1, g_2 be the resulting strand diagrams. Consider the universal cover of the annulus, with the iterated preimage of the annular strand diagram drawn upon it. Any path σ in the annulus lifts to a collection $\{\sigma^{(i)} : i \in \mathbb{Z}\}$ of disjoint paths in the universal cover:

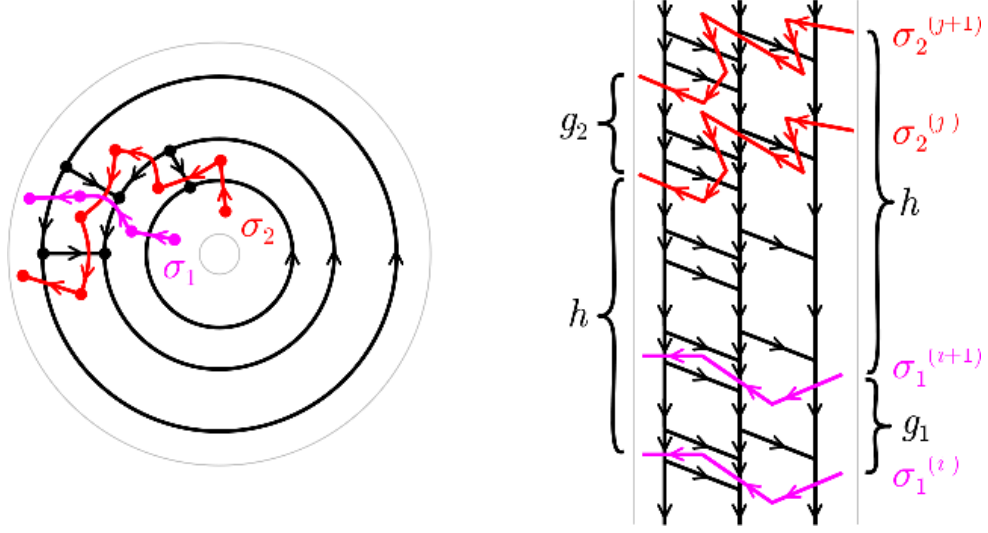


Figure 2.12: Creating a conjugator

Then $g_1 h = h g_2$, where h is the strand diagram bounded by $\sigma_1^{(i)}$ and $\sigma_2^{(j)}$ for some $j \gg i$, that is we choose j big enough so that the two paths $\sigma_1^{(i)}$ and $\sigma_1^{(i+1)}$ do not intersect any of the two paths $\sigma_2^{(j)}$ and $\sigma_2^{(j+1)}$ (see figure 2.12). Assume now that g_1 and g_2 are, respectively, (k, k) -strand diagram and an (m, m) -strand diagram. We have proved that they are conjugate in Thompson's groupoid \mathcal{F} (see Note 2.1.3). To conclude the proof we can rewrite g_1, g_2, h as $(1, 1)$ -strand diagrams using the right vine, that is

$$v_k g_1 v_k^{-1} (v_k h v_m^{-1}) = (v_k h v_m^{-1}) v_m g_2 v_m^{-1}. \quad \square$$

Therefore, any annular strand diagram determines a conjugacy class in F .

Proposition 2.1.11. *Equivalent strand diagrams determine the same conjugacy class.*

Proof: Recall that a type III reduction is the composition of a type II reduction and an inverse reduction of type I. Therefore, it suffices to show that the conjugacy class is unaffected by reductions of types I and II.

Given any reduction of type I or type II, it is possible to find a cutting path that does not pass through the affected area. In particular, any cutting path that passes through the area of reduction can be moved (figure 2.13).

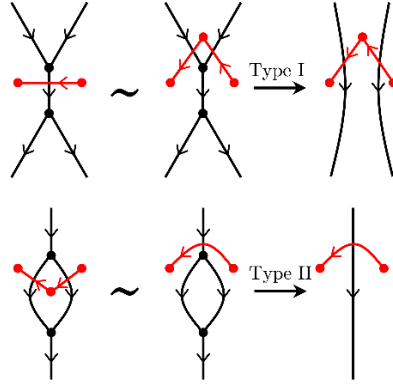


Figure 2.13: Moving the cutting path past the reduction area

If we cut along this path, then we are performing a reduction of the resulting strand diagram, which does not change the corresponding element of F . \square

This proves Theorem 2.1.9. The reduced annular strand diagram is a computable invariant, so this gives a solution to the conjugacy problem in F . We will discuss in Section 2.4 that the complexity of this algorithm can be implemented in linear time.

2.1.4 Structure of Annular Strand Diagrams

Figure 2.14 shows an example of a reduced annular strand diagram.

The main feature of this diagram is the large directed cycles winding counterclockwise around the central hole. We begin by analyzing the structure of these cycles:

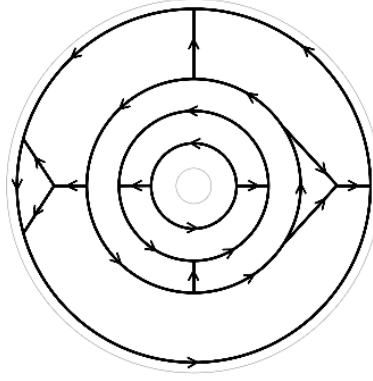


Figure 2.14: A reduced annular strand diagram

Proposition 2.1.12. *Let L be a directed cycle in a reduced annular strand diagram. Then either:*

1. *L is a free loop, or*
2. *Every vertex on L is a split, or*
3. *Every vertex on L is a merge.*

Proof: Suppose L has both splits and merges. Then if we trace around L , we must eventually find a merge followed by a split, implying that the annular strand diagram is not reduced. \square

We shall refer to L as a *split loop* if its vertices are all splits, and as a *merge loop* if its vertices are all merges.

Proposition 2.1.13. *For any reduced annular strand diagram:*

1. *Any two directed cycles are disjoint, and no directed cycle can intersect itself.*
2. *Every directed cycle winds exactly once around the central hole. Hence, any cutting path intersects each directed cycle exactly once.*

3. *Every component of the graph has at least one directed cycle.*
4. *Any component with only one directed cycle is a free loop.*
5. *By following the cutting path within a component, it is possible to order all the directed cycles touched by the path. This order is independent of the choice of the cut. Moreover, these concentric cycles must alternate between merge loops and split loops.*

Remark 2.1.14. In the next Chapter we will analyze again in more detail the connection between strand diagrams and piecewise linear functions. The order of directed loops defined in part 5 of Proposition 2.1.13 follows naturally from the order of the unit interval. Compare with Theorem 3.2.6.

Proof: For statement (1), observe that intersecting directed cycles would have to merge together and then subsequently split apart, implying that the diagram is not reduced. For (2), recall that the directed cycles are required to wind around at least once, and, since the graph is embedded in the plane, any closed curve that wound around more than once would have a self-intersection.

For (3), observe that any vertex in an annular strand diagram has at least one outgoing edge, and therefore any directed path can be extended indefinitely. If we start a path at a vertex p , then the path must eventually intersect itself as there are only finitely many vertices in the component, which proves the existence of a directed loop in the component containing p .

For (4), suppose that a component of an annular strand diagram has a split loop. Any path that begins at a split can never again intersect the split loop, and must therefore eventually intersect a merge loop, proving that this component

has at least two directed cycles. Similarly, any path followed backwards from a merge loop must eventually intersect a split loop.

For (5), observe that two adjacent concentric directed cycles in the same component cannot both be split loops: a path starting in the region between them must eventually cycle, for it cannot end on any of the two split loops. Similarly, it is not possible to have two concentric merge loops. To prove that the order does not depend on the cutting path we start by observing that, by the proof of Proposition 2.1.10, any two cutting paths bound a conjugator h in Thompson's groupoid. By Proposition 7.2.1 in [5], h must be a product of merges and splits, so to conclude we must observe that if one cutting path can be obtained from another by passing through a merge or a split, the order of directed cycles does not change. This is immediately clear by looking at the moves in figure 2.13. \square

In the next section we will define *cylindrical strand diagrams* for elements of Thompson's group T . With this definition and the previous proposition, we can construct a component of a reduced annular strand diagram by drawing alternating split and merge loops, and then filling the connections between them with unlabeled reduced cylindrical strand diagrams (see figure 2.15).

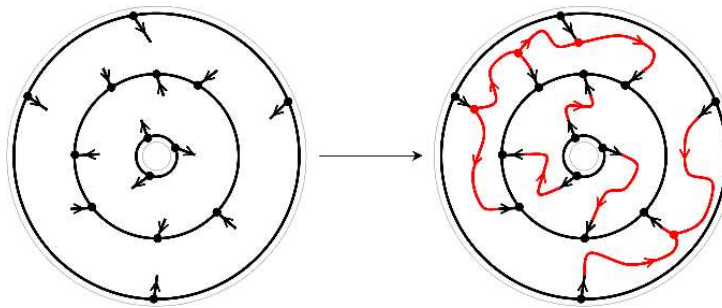


Figure 2.15: Constructing an annular strand diagram

A general reduced annular strand diagram consists of several concentric

rings, each of which is either a free loop or a component of this form.

2.2 Conjugacy in Thompson's group T

2.2.1 Strand Diagrams for T

We are now going to generalize to Thompson's group T the diagrams and the characterization of conjugacy that we have found for F . As many parts of this section are similar to the previous one, we are going to omit some details to avoid repetition. A *cylindrical strand diagram* is a strand diagram drawn on the cylinder $S^1 \times [0, 1]$, instead of on the unit square (figure 2.16).

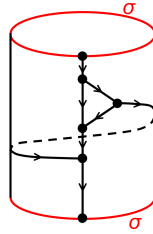


Figure 2.16: A cylindrical strand diagram

As with strand diagrams on the square, isotopic cylindrical strand diagrams are considered equal. We remark that isotopies of the cylinder include Dehn twists. We recall that a *Dehn twist* of the cylinder is a homeomorphism obtained by holding the top circle rigid while rotating the bottom circle through an angle of 2π . Hence two diagrams are equal if we can get from one to the other through a Dehn twist on the bottom. A *reduction* of a cylindrical strand diagram is either of the moves shown in figure 2.17.

For the second move, the two parallel edges are required to span a disc on

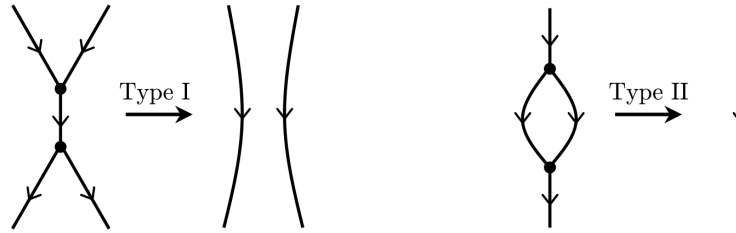


Figure 2.17: Reductions for a cylindrical strand diagram

the cylinder. In particular, the diagram shown in figure 2.18 cannot be reduced.

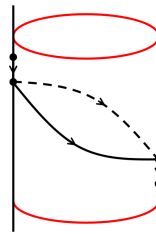


Figure 2.18: A cylindrical strand diagram that is not reducible

Any cylindrical strand diagram is equivalent to a unique reduced cylindrical strand diagram. Cylindrical strand diagrams represent elements of Thompson's group T . Given an element of T , we can construct a cylindrical strand diagram by attaching the two trees of the tree diagram along corresponding leaves (figure 2.19).

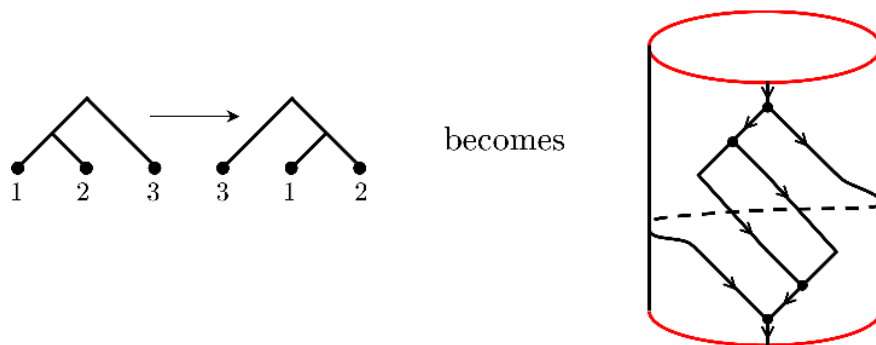


Figure 2.19: From a tree diagram to a cylindrical strand diagram

Conversely, we can cut any reduced cylindrical strand diagram along all the

edges that go from a split to a merge. This cuts the diagram into two trees, each of which is contained in its own cylinder (figure 2.20).

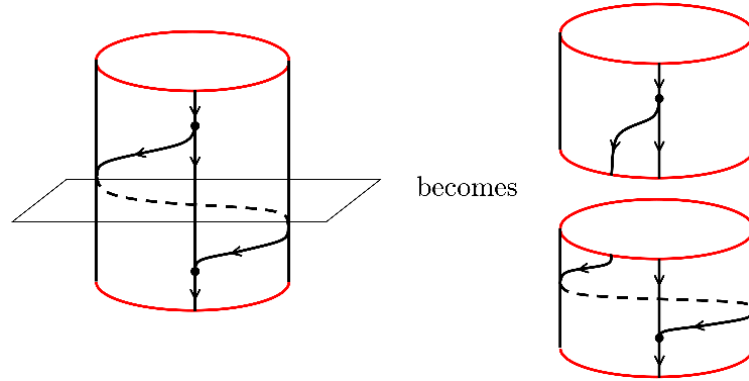


Figure 2.20: From a cylindrical strand diagram to a tree diagram

The leaves of each tree lie along a circle, and therefore the correspondence between the leaves must be a cyclic permutation.

Note 2.2.1. There is a slight difficulty in the definition of cylindrical (m, n) -strand diagrams (figure 2.21).

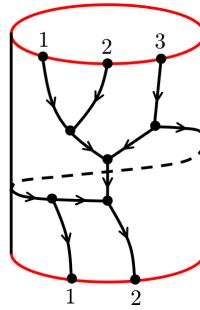


Figure 2.21: An (m, n) -strand diagram

If we want concatenation of cylindrical (m, n) -strand diagrams to be well-defined, we must insist on a labeling of the sources and sinks (as in the figure above). Assuming this requirement, the set of cylindrical (m, n) -strand diagrams forms a groupoid, with the group based at 1 being Thompson's group T . Using

the canonical embedding of the right vine on a cylinder, we can then view any cylindrical (m, n) -strand diagram as representing an element of T .

2.2.2 Characterization of Conjugacy in T

If we glue together the top and bottom of a cylindrical strand diagram, we obtain a strand diagram on the torus. The common image of the top and bottom circles is called a *cutting loop*.

Definition 2.2.2. A *toral strand diagram* is a directed graph embedded on the torus $S^1 \times S^1$ with the following properties:

1. Every vertex is either a merge or a split.
2. Every directed cycle has positive index around the central hole.

To make the second requirement precise, let c be the cohomology class $(1, 0)$ in $H^1(S^1 \times S^1) = \mathbb{Z} \times \mathbb{Z}$. Then a toral strand diagram is required to satisfy the condition $c(\ell) > 0$ for every directed loop ℓ . For a toral strand diagram obtained from a cylinder, c is precisely the cohomology class determined by counting intersection number with the cutting loop. For this reason, we shall refer to c as the *cutting class*.

The cutting class is related to a slight difficulty in defining the notion of equality for toral strand diagrams. Because a Dehn twist of the cylinder is isotopic to the identity map, two cylindrical strand diagrams that differ by a Dehn twist are isotopic and hence considered equal. However, the resulting toral strand diagrams are not isotopic (for example, see figure 2.22).

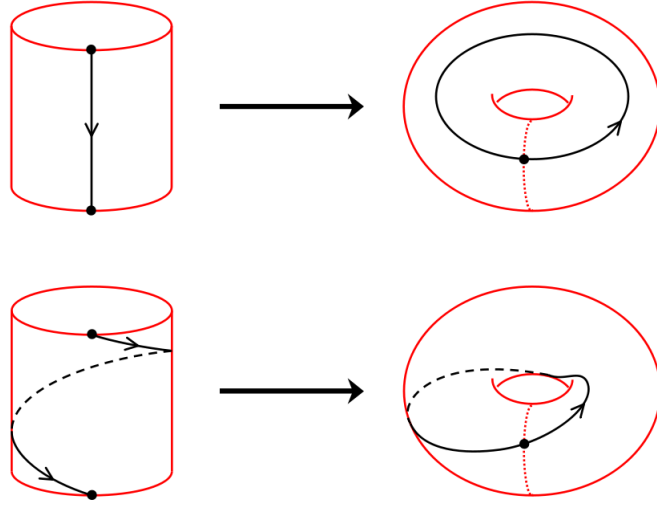


Figure 2.22: Toral strand diagrams that are not isotopic

This difficulty arises because the Dehn twist descends to a nontrivial homeomorphism of the torus (i.e. a homeomorphism that is not isotopic to the identity). Using the standard basis for the first cohomology group of the torus (since $c = (1, 0)$), this Dehn twist acts as $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Therefore, we must consider two toral strand diagrams equal if their isotopy classes differ by a Dehn twist of the form $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. This is equivalent to the following convention:

Convention 2.2.3. Let S_1 and S_2 be two strand diagrams embedded on the torus \mathbb{T} . We say that S_1 and S_2 are *equal* if there exists an orientation-preserving homeomorphism $h: \mathbb{T} \rightarrow \mathbb{T}$ such $h^*(c) = c$ and $h(S_1) = S_2$.

Definition 2.2.4. A *cutting loop* for a toral strand diagram is a simple continuous loop in the torus that satisfies the following conditions:

1. The loop is dual to the cohomology class c .
2. The loop does not pass through any vertices of the strand diagram.

3. The loop intersects edges of the strand diagram transversely, with the orientation shown in figure 2.23.

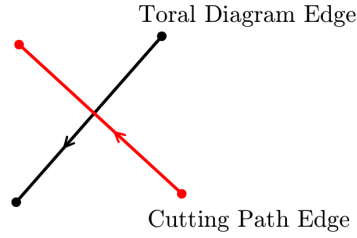


Figure 2.23: Orientation of the cutting class

Proposition 2.2.5. *Cutting a toral strand diagram along a cutting loop yields a (k, k) -strand diagram embedded on the cylinder. \square*

Theorem 2.2.6. *Every toral strand diagram has a cutting loop. \square*

Definition 2.2.7. A reduction of a toral strand diagram is any of the three types of moves shown in figure 2.24

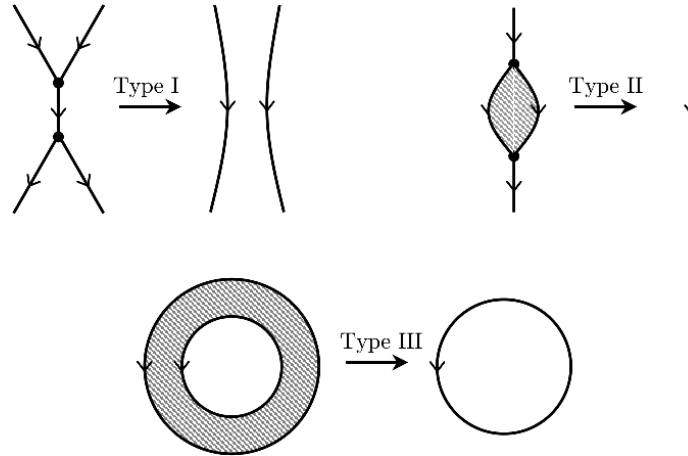


Figure 2.24: Reductions for a toral strand diagram

In the second move, the two edges of the bigon are required to span a disc, and in the third move the two loops must be the boundary of an annular region.

Two toral strand diagrams are *equivalent* if one can be obtained from the other via a sequence of reductions and inverse reductions.

Proposition 2.2.8. *Every toral strand diagram is equivalent to a unique reduced toral strand diagram.*

Proof: The argument on reductions used in the proof of Proposition 2.1.8 can be extended to this case without additional details and so we omit it. \square

Gluing the top and the bottom circles of a cylindrical strand diagram is not well defined in general. However by Convention 2.2.3, all resulting toral diagrams are equal.

Theorem 2.2.9. *Two elements of T are conjugate if and only if they have the same reduced toral strand diagram.*

Proof: Our convention for equality of strand diagrams guarantees that any two conjugate elements of T yield the same reduced toral strand diagram.

We claim that any two cutting loops for the same toral strand diagram yield conjugate elements of T . Suppose we are given cutting loops ℓ_1 and ℓ_2 , and consider the cover of the torus corresponding to the subgroup $\ker(c) \leq \pi_1(\mathbb{T})$. This cover is an infinite cylinder, with the deck transformations $\pi_1(\mathbb{T})/\ker(c) \cong \mathbb{Z}$ acting as vertical translation. Each of the loops ℓ_i lifts to an infinite sequence $\{\ell_i^{(j)}\}_{j \in \mathbb{Z}}$ of loops in this cover, and the region between $\ell_i^{(j)}$ and $\ell_i^{(j+1)}$ is the cylindrical strand diagram f_i obtained by cutting the torus along ℓ_i . It follows that $f_1 g = g f_2$, where g is the cylindrical strand diagram between $\ell_1^{(j)}$ and $\ell_2^{(k)}$ for some $k \gg j$.

Clearly reductions do not change the conjugacy class described by a toral

strand diagram, and therefore any two elements of T with the same reduced toral strand diagram are conjugate. \square

2.2.3 Structure of Toral Strand Diagrams

The following section is an analogue for T of Section refsec:structure-annular-diagrams for F . Given an element $f \in T$, the structure of the toral strand diagram for f is closely related to the dynamics of f as a self-homeomorphism of the circle. In this section we analyze the structure of toral strand diagrams, and in the next we show how this structure is related to the dynamics of an element.

We begin by noting some features of annular strand diagrams that remain true in the toral case:

Proposition 2.2.10. *For any reduced toral strand diagram.*

1. *Any directed cycle is either a free loop, a split loop, or a merge loop.*
2. *Any two directed cycles are disjoint, and no directed cycle can intersect itself.*
3. *Every component of the graph has at least one directed cycle, and any component with only one directed cycle is a free loop. \square*

In an annular strand diagram, each directed cycle winds around the central hole exactly once, and the components of the diagram form concentric rings. The structure of a toral strand diagram is more complicated.

Proposition 2.2.11. *Let $c \in H^1(\mathbb{T})$ denote the cutting class. Without loss of generality, we can assume that $c = (1, 0)$. Then any two directed cycles represent the same element $(n, k) \in H_1(\mathbb{T})$, where $n > 0$ and k and n are relatively prime.*

Proof: By the definition of a toral strand diagram, $n > 0$ for any directed cycle. Any two disjoint nontrivial loops on a torus are homotopic, and therefore any two directed cycles must have the same (n, k) . Furthermore, since a directed cycle cannot intersect itself, n and k must be relatively prime. \square

Note that the number k is not uniquely determined. Specifically, recall that two strand diagrams that differ by the Dehn twist $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ are equal. (This matrix is the transpose of the earlier matrix, since we are now considering the action on homology.) Applying this Dehn twist to a diagram whose directed cycles are (n, k) yields a diagram whose cycles are $(n, k + n)$, so the number k is only well-defined modulo n .

We will always assume that $0 \leq k < n$. The reduced fraction $k/n \in [0, 1)$ is called the *rotation number* of a toral strand diagram. It is possible to show that this corresponds to the dynamical rotation number of a homeomorphism $f \in T$ (see Chapter 6 for the definition).

Proposition 2.2.12 (Ghys-Sergiescu, [31]). *Every element of T has a periodic point.*

Proof. We delay this proof to Section 3.1.3. See Proposition 3.1.3. \square

We remark that the previous result has been recently proved again by Calegari in [24]. Bleak and Farley [8] also have a proof of this result using “revealing tree-pair diagrams” as introduced by Brin [15].

Proposition 2.2.13 (Burillo-Cleary-Stein-Taback, [21]). *For any positive integer n , let c_n be the (n, n) -strand diagram. Then any torsion element of T is conjugate to a power of some $v_n^{-1} c_n v_n$ for some integer n .*

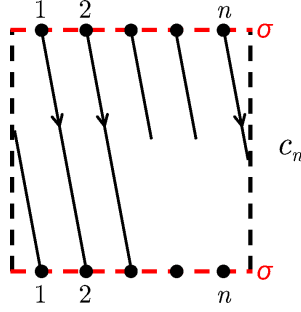


Figure 2.25: The torsion element c_n

Proof. If $f \in T$ is torsion, then f cannot have any merge or split loops. Hence the reduced toral strand diagram for f has only free loops. By opening the reduced toral strand diagram through the cutting line, we obtain a strand diagram which is a power c_n^k for some n . We can obtain the corresponding $(1, 1)$ -strand diagram by writing $v_n^{-1} c_n^k v_n$. \square

It is not too hard to see that, for any $1 \leq k < n$, the element c_n^k has rotation number k/n . This proves that, for any rational number $k/n \pmod{1}$ there is an element of T with rotation number k/n (another result due to Ghys and Sergiescu in [31]).

2.3 Conjugacy in Thompson's group V

2.3.1 Strand Diagrams for V

Definition 2.3.1. An *abstract strand diagram* is an acyclic directed graph, together with a cyclic ordering of the edges incident on each vertex, and subject to the following conditions:

1. There exists a unique univalent source and a unique univalent sink.
2. Every other vertex is either a split or a merge.

The cyclic orderings of the edges allow us to distinguish between the left and right outputs of a split, and between the left and right inputs of a merge. We can draw an abstract strand diagram as a directed graph in the plane with edge crossings (see figure 2.26).

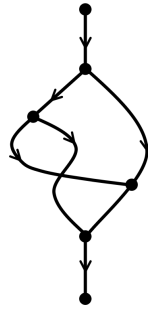


Figure 2.26: An abstract strand diagram

By convention, the edges incident on a vertex are always drawn so that the cyclic order is counterclockwise. Reductions in this setting are defined via the drawing of the graph in the plane, because we need the vertices to be oriented in the same way of the plane. A *reduction* of an abstract strand diagram (drawn in the plane) is either of the moves of figure 2.27.

The first two moves are the same kind of move, drawn differently depending on the embedding in the plane. The cyclic order of the vertices must be exactly as shown above. The move shown in figure 2.28 is not valid.

Every abstract strand diagram is equivalent to a unique reduced abstract strand diagram. Abstract strand diagrams represent elements of Thompson's group V . Given an element $f \in V$, we can construct an abstract strand diagram

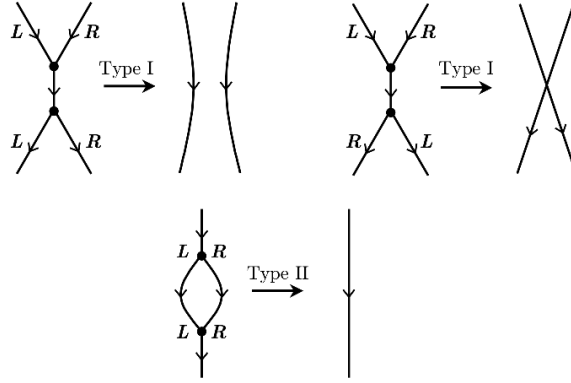


Figure 2.27: Reductions for abstract strand diagrams

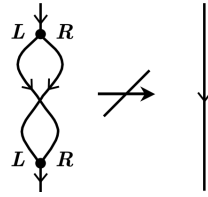


Figure 2.28: Non valid reduction.

for V by attaching the two trees of a tree diagram for f along corresponding leaves (figure 2.29).

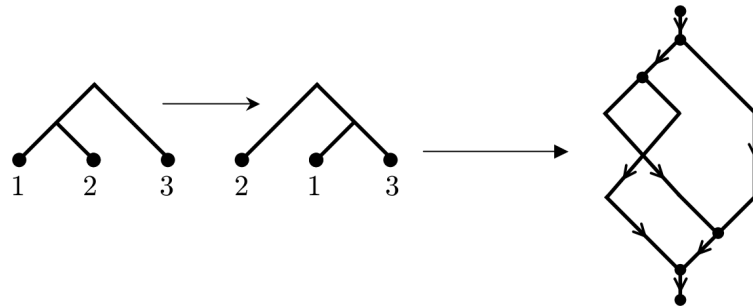


Figure 2.29: From a tree diagram to an abstract strand diagram

Conversely, any reduced abstract strand diagram can be cut along all the edges that go from splits to merges to yield a tree diagram. Assuming we label the sources and sinks, the set of abstract (m, n) -strand diagrams forms a groupoid, and elements of this groupoid can be viewed as representing elements

of Thompson's group V .

2.3.2 Characterization of Conjugacy in V

If we glue together the sources and sinks of an abstract strand diagram, we obtain a directed graph whose vertices are all merges and splits. The images of the original sources and sinks now fall in the interiors of certain edges, and are called the *cut points*. Note that a single edge may contain more than one cut point. The function that measures the number of cut points in each edge is a 1-cocycle, and therefore yields a cohomology class c , which we call the *cutting class*.

Definition 2.3.2. A *closed strand diagram* is a triple (D, o, c) , where

1. D is a directed graph composed of splits and merges,
2. o is a cyclic ordering of the edges around each vertex of D , and
3. c is an element of $H^1(D)$ satisfying $c(\sigma) > 0$ for every directed cycle σ .

The cohomology class c is called the *cutting class*. To make our arguments as accessible as possible, we will use a very geometric approach to cohomology. In particular, we will make heavy use of the following well known result: for any CW-complex X , there is a natural one-to-one correspondence between elements of $H^1(X)$ and homotopy classes of maps from X to the punctured plane. Using the above theorem, we can represent a closed strand diagram as a graph with crossings drawn on the punctured plane (figure 2.30).

The cohomology class c is given by winding number around the puncture.

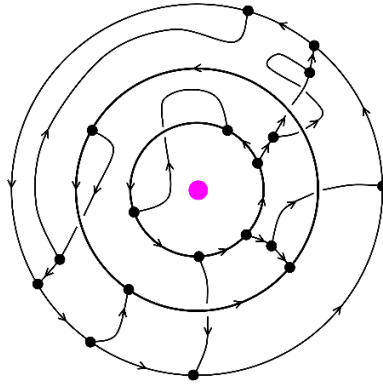


Figure 2.30: A closed strand drawn on the punctured plane

By convention, we always draw closed strand diagrams so that the cyclic order of the edges around each vertex is counterclockwise.

Definition 2.3.3. Given a drawing of a closed strand diagram, a *cutting line* is a continuous path going from the center to the outer region so that it does not intersect any vertex but it intersects the edges of the diagram transversely, with the orientation shown in figure 2.31

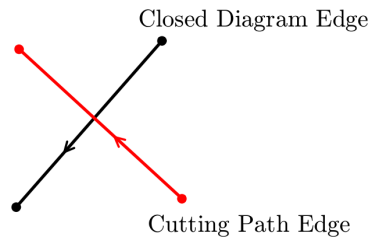


Figure 2.31: Orientation of the cutting class

The sequence p_1, \dots, p_n of points on the graph cut by the line is called a *cutting sequence*. Note that we can “cut” along a cutting sequence to obtain an ordered abstract (k, k) -strand diagram. The above definition is very geometric. Here is a combinatorial description of cutting sequences:

Proposition 2.3.4. *Let p_1, \dots, p_n be a sequence of points lying in the interiors of the edges of a closed strand diagram. Then p_1, \dots, p_n is a cutting sequence if and only if the function*

$$e \mapsto \#\{i : p_i \in e\}$$

is a 1-cochain representing the cutting class c . \square

Theorem 2.3.5. *Every closed strand diagram has a cutting sequence.*

Proof: From theorem A.1.1 in the appendix, there exists a non-negative, integer-valued cochain α representing c . Then the sequence p_1, \dots, p_n can be constructed by choosing $\alpha(e)$ points from each edge e . \square

Definition 2.3.6. A *reduction* of a closed strand diagram is any of the three moves shown in figure 2.32.

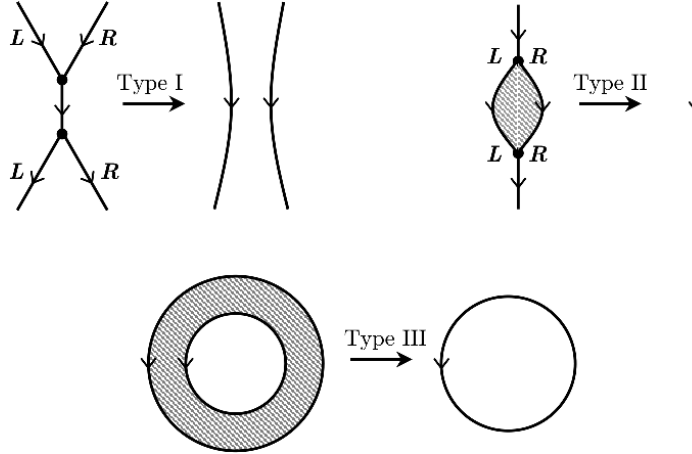


Figure 2.32: Reductions for closed strand diagrams

In the second move, the loop spanned by the bigon must lie in the kernel of c , i.e. the parallel edges must be homotopic in the punctured plane. In the third move, we require that the difference of the two loops lie in the kernel of c ,

or equivalently that the two loops have the same winding number around the puncture.

In each of the three cases, the reduced graph D' inherits a cutting class in the obvious way. For a type I reduction, the new cutting class is $\varphi^*(c)$, where φ is the obvious map $D' \rightarrow D$ (figure 2.33).

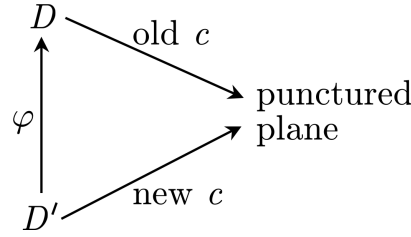


Figure 2.33: Cutting classes and reductions

For a reduction of type II, there are two obvious maps $D' \rightarrow D \rightarrow \{\text{punctured plane}\}$: we send the reduced edge to any of the two sides of the bigon. These maps are homotopic, and therefore yield the same homomorphism $H^1(D) \rightarrow H^1(D')$. The same holds for reductions of type III.

Proposition 2.3.7. *Every closed strand diagram is equivalent to a unique reduced closed strand diagram.*

Proof: We must show that reduction is locally confluent, keeping careful track of the fate of the cohomology class c . Suppose that a single closed strand diagram is subject to two different reductions. If one of these reductions is of type III or they remove disjoint sets of vertices, then they commute. If the reductions share a single vertex, then the results of the two reductions are the same, as seen in previous cases (see figure 2.11 in Proposition 2.1.8). Note in particular that the map $D' \rightarrow D$ obtained from the type I reduction is homotopic in the punctured plane to the pair of maps $D' \rightarrow D$ obtained from the type II reduction. Finally, it

is possible for the reductions to involve the same pair of vertices, in which case they can be resolved with a reduction of type III (figure 2.34).

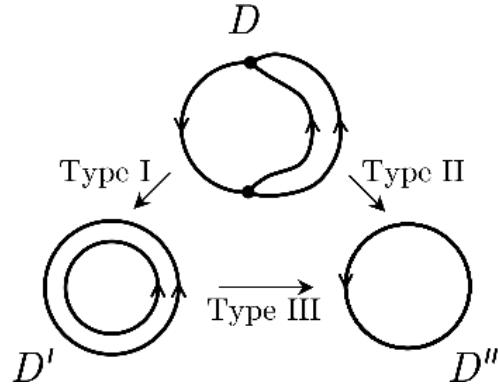


Figure 2.34: Diamond Lemma

Again, observe that the two maps $D'' \rightarrow D$ obtained from the type II reduction are homotopic to the two composite maps $D'' \rightrightarrows D' \rightarrow D$. \square

Lemma 2.3.8. *Conjugate elements of V yield isomorphic reduced closed strand diagrams.*

Proof. Let $f, g \in V$. Then figure 2.35 is a closed strand diagram for both f and $g^{-1}fg$.

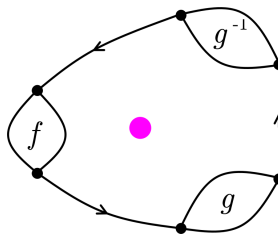


Figure 2.35: Same reduced closed strand diagram

Since f and $g^{-1}fg$ share a closed strand diagram, they must have the same reduced closed strand diagrams. \square

Theorem 2.3.9. *Two elements of V are conjugate if and only if they have isomorphic reduced closed strand diagram.*

Proof: We claim that any two cutting sequences $\{p_1, \dots, p_m\}, \{q_1, \dots, q_n\}$ for isomorphic closed strand diagram S yield conjugate elements of V . Consider the infinite-sheeted cover of the strand diagram obtained by lifting to the universal cover of the punctured plane. (Abstractly, this is the cover corresponding to the subgroup $\ker(c)$ of $\pi_1(D)$.) If we arrange S on the punctured plane so that the points $\{p_1, \dots, p_n\}$ lie on a single radial line ℓ , then the lifts of this line cut the cover into infinitely many copies of the abstract strand diagram f obtained by cutting S along $\{p_1, \dots, p_n\}$. Specifically, the points $\{p_1, \dots, p_m\}$ have lifts $\{p_1^{(i)}, \dots, p_m^{(i)}\}_{i \in \mathbb{Z}}$, with the i th copy of f having $\{p_1^{(i)}, \dots, p_m^{(i)}\}$ as its sources and $\{p_1^{(i+1)}, \dots, p_m^{(i+1)}\}$ as its sinks. Similarly, if we homotope S so that $\{q_1, \dots, q_n\}$ lie on a single radial line, we obtain a decomposition of the cover into pieces isomorphic to the abstract strand diagram g obtained by cutting S along $\{q_1, \dots, q_n\}$. It follows that $fh = hg$, where h is the abstract strand diagram lying between $\{p_1^{(i+1)}, \dots, p_m^{(i+1)}\}$ and $\{q_1^{(j)}, \dots, q_n^{(j)}\}$ for some $i \ll j$. \square

2.3.3 Structure of Abstract Closed Strand Diagrams

Most of the results seen before, generalize to this setting. For example, reduced abstract closed strand diagram have the same combinatorial structure as toral strand diagrams (i.e. They must contain a directed cycle, all cycles must be disjoint, etc.).

Theorem 2.3.10 (Brin, [15]). *Let $f \in V$, then:*

1. f has a periodic point.
2. If f is torsion, it is conjugate to a permutation.
3. There is an integer $n(f)$ so that every finite orbit of f has no more than $n(f)$ elements.

Proof. (i) follows along the same lines as Proposition 2.2.12. (ii) follows along the same lines as Proposition 2.2.13. For (iii) we recall that the reduced tree diagram of f gives a partition of the interval $[0, 1]$ and let p be a point in a finite orbit. Then p is in some interval $[a, b]$ of the partition and there is a power f^k such that f^k sends $[a, b]$ into itself, and so the abstract closed strand diagram has a directed cycle passing through the vertex corresponding to $[a, b]$. Thus the orbit of p cannot have more than k points, where k is the length of the cycle containing $[a, b]$. Thus the length of any finite orbit is bounded by $n(f)$ maximum length of a directed cycle of the abstract closed strand diagram. \square

2.3.4 Generalizations and Conjectures

It seems possible to take this unified point of view and generalize it to a more abstract setting. We start by conveying an intuition. We observe that, in the case of F , diagrams were embedded in the unit square $I \times I$ while in the case of T they were embedded in the cylinder $S^1 \times I$. Similarly, diagrams in V could be regarded as embedded in the space $\mathbb{R}^3 \times I$. We can try to define strand diagrams embedded in a space $M \times I$ where M is a suitable space (for example, a differentiable manifold or a CW-complex). However, issues arise when we try to define reductions since isotopy can move the cyclic ordering of a vertex and switch left

with right. We remember that all of our definitions of reductions took place on a particular surface.

One can define *ribbon surfaces* instead of strand diagrams. They are diagrams obtained by “fattening” a strand diagram to become an orientable surface with boundary. More precisely, we can take an abstract strand diagram as defined in V and embed it in $M \times I$ so that the source is the unique point contained in $M \times \{0\}$ and the sink is the unique point contained in $M \times \{1\}$, then we attach the following *ribbon splits* and *ribbon merges* at each vertex (see figure 2.36).

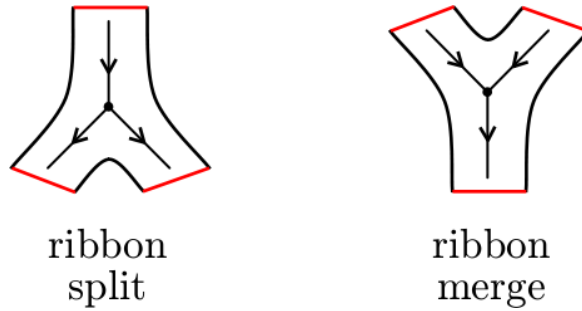


Figure 2.36: Ribbon splits and merges

We can complete the surface by attaching rectangles along the edges and gluing them on the inputs and the outputs of the ribbon splits and merges. Now we have a well defined surface inside $M \times I$ and we can orient it, starting from the top. We can still talk about “trivalent parts” of the surface, to mean the corresponding “vertices” of this surface. We can now define isotopy and equivalence of the surface inside $M \times I$ and define a product of surfaces. Finally we can define reductions of a surface: they will be defined by the motions shown in figure 2.37.

where the depicted pieces of the ribbon surface are assumed to have been embedded in the plane, according to the orientation of these pieces. We observe

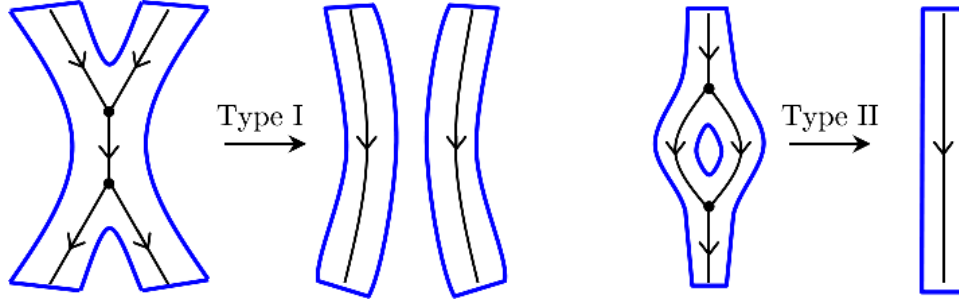


Figure 2.37: Ribbon reductions

that the second reduction assumes that there exists a 2-cell contained in $M \times I$ that can be attached to the ribbon surface and whose interior does not intersect the ribbon surface at any point. We can continue this line of thinking by defining *closed ribbon surfaces* inside the space $M \times S^1$, by gluing the ends of a ribbon surface in $M \times I$. We can thus define a third kind of reduction if we can glue two circular strips by another circular strip that is entirely contained in $M \times S^1$ and whose interior does not intersect the ribbon surface at any point.

It is still possible to prove that each of the closed diagrams is equivalent to a unique reduced diagram and that any two conjugate ribbon surfaces in $M \times I$ give rise to the same reduced closed ribbon surface. Proving the converse seems also possible, although it will depend on the properties of the space M , however, one can still theoretically follow the “infinite sheeted cover” argument and try to prove it in this setting.

Using this new generalization, if we choose the space M to be \mathbb{R}^2 we get a group of ribbon surfaces which resembles the braided Thompson’s group BV . Brin has studied some properties and presentations of Thompson’s group BV in the paper [17] while Burillo and Cleary have described some of its metric properties in [22]. The descriptions given previously by Brin and Burillo were

describing elements as as pairs of trees with a braid connecting the leaves (see figure 2.38).

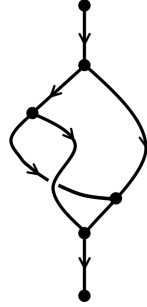


Figure 2.38: An element of Thompson's group BV

It would be interesting to study the particular case of ribbon surfaces in $\mathbb{R}^2 \times I$. Our procedure is a generalization of the point of view of binary tree diagrams for Thompson's groups. However, one could extend it to define strand diagrams in $M \times I$ where all the vertices are n -ary splits and merges to recover the same conjugacy results for higher dimensional Thompson's groups as defined by Brin in [15].

We want to conclude this section, by describing another tempting generalization. Guba and Sapir have introduced a class of groups called *diagram groups* in their monograph [38]. These groups are defined by elements that can be represented as diagrams in the plane and Thompson's group F can be described as one such group. Our solution of the conjugacy problem for F is heavily inspired by and similar to the one they give for diagrams groups. Guba and Sapir describe other families of diagram groups that live in other spaces and they recover T and V inside these classes. They suggest that their work could be extended to diagram groups in these settings.

It is possible to define general *ribbon-diagram groups* in $M \times I$ and it would be

interesting to see if their solution for the conjugacy problem could be extended to this general setting.

Conjecture 2.3.11. The strategy to solve the conjugacy problem for strand diagram groups can also be used to solve the conjugacy problem for ribbon-diagram groups defined in $M \times I$.

2.4 Running Time

In this section, we study the complexity of our solution of the conjugacy problem for Thompson's groups F, T and V . We start by sketching a proof of the following result:

Theorem 2.4.1. *There exists a linear-time algorithm to determine whether two elements of F are conjugate.*

We assume that the two elements of F are given as words in the generating set $\{x_0, x_1\}$. "Linear time" means that the algorithm requires $O(N)$ operations, where N is the sum of the lengths of these words. We shall use the algorithm of Hopcroft and Wong (see [41]):

Theorem 2.4.2 (Hopcroft and Wong). *There exists a linear-time algorithm to determine whether two planar graphs are isomorphic. \square*

We remark that Guba and Sapir had already proven that their solution to the conjugacy problem for diagram groups had the same complexity of the isomorphism problem for planar graphs (private communication). Thus their solution along with Theorem 2.4.2 give again a linear time algorithm.

Proposition 2.4.3. *There exists a linear-time algorithm to determine whether two (reduced) annular strand diagrams are isotopic.*

Proof: We must show that isotopy of connected annular strand diagrams reduces to isomorphism of planar graphs in linear time. If the given strand diagrams are disconnected, then we may check isotopy of the components separately. It therefore suffices to prove the proposition in the connected case. Given a strand diagram, subdivide each edge into three parts, and attach new edges around each merge and split as drawn in figure 2.39.

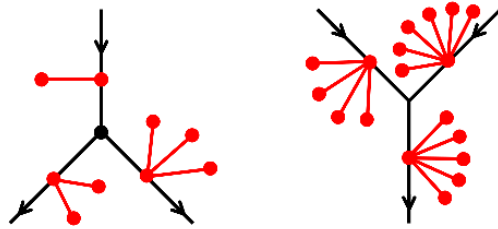


Figure 2.39: Decorating the annular strand diagram.

This new graph can be constructed in linear time, and its isomorphism type completely determines the isotopy class of the original reduced annular strand diagram. In particular, the decorations determine both the directions of the original edges and the cyclic order of the original edges around each merge or split.

□

All that remains is to show that the reduced annular strand diagram for an element of F can be constructed in linear time. This requires two steps:

1. Construct a strand diagram for the element.
2. Reduce the resulting annular strand diagram.

The first step is easy to carry out in linear time: given a word in $\{x_0, x_1\}$, simply concatenate the corresponding strand diagrams for the generators and their inverses. No reduction is necessary in this phase. For the second step, observe that any reduction of a strand diagram reduces the number of vertices, and therefore only linearly many reductions are required. However, it is not entirely obvious how to search for these reductions efficiently.

Proposition 2.4.4. *Suppose that any one reduction can be performed in constant time. Then a given annular strand diagram G can be reduced in linear time.*

Proof: We give a linear-time algorithm for performing all the necessary type I and type II reductions. Any required type III reductions can be performed afterwards.

We can write G as a set of vertices $V = \{v_1, \dots, v_k\} := V_1$. We build inductively new sets of vertices V_i . To build the sequence V_{i+1} , we read and classify every vertex of V_i . We let R_i be the set of vertices of V_i which are reducible. By definition R_i will have an even number of vertices, since a vertex is reducible if there is an adjacent vertex which forms a reduction in the diagram. Then we define V_{i+1} to be all the vertices of $V \setminus \left(\bigcup_{j=1}^i R_j\right)$ which are adjacent to a vertex in R_i .

This algorithm goes to look for vertices which were not reducible at the i -th step, but might have become reducible at the $i+1$ -th step. We repeat this process until we find an m such that $R_m = \emptyset$. By construction,

$$|R_{i+1}| \leq |V_{i+1}| \leq 4|R_i|$$

since every point involved in a reduction is adjacent to at most 3 vertices, one of which will be reduced. In other words, for each pair of vertices that we reduce, we might have to reinsert up to 4 vertices which were previously not reducible.

On the other hand, it is obvious that

$$\sum_{i=1}^m |R_i| \leq |V|.$$

The final cost of the computation is thus given by

$$\sum_{i=1}^m |V_i| = |V| + \sum_{i=1}^m |V_{i+1}| \leq |V| + 4 \sum_{i=1}^m |R_i| \leq |V| + 4|V| = 5|V|. \quad \square$$

Though it may seem that we are done, we have not yet specified the time needed to perform a reduction. To do this we must choose a specific data structure to represent an annular strand diagram, and this choice is fraught with difficulty. We have worked out the details, and it suffices to keep track of either the dual graph (i.e. the cell structure) or of the sequence of edges crossed by some cutting path. In neither case can reductions actually be performed in constant time, but one can show that the amount of time required for linearly many reductions is indeed linear.

Unfortunately, the algorithm may not be as fast for the groups T and V . Checking whether two closed strand diagrams are the same involves a comparison of the cutting cohomology classes. This requires a Gaussian elimination, for it must be determined whether the difference of the two classes lies in the subspace spanned by the coboundaries of the vertices. Gaussian elimination has cubic running time, thus:

Theorem 2.4.5. *Let X be Thompson's group T or V described through their standard generating sets. There exists a cubic time algorithm to determine whether two elements of X are conjugate.*

CHAPTER 3

DYNAMICS IN THOMPSON'S GROUP F

In Chapter 2, we used *strand diagrams* to give a unified solution to the conjugacy problems in Thompson's groups F , T , and V . In the present Chapter, we derive an explicit correspondence between strand diagrams for F ¹ and piecewise-linear functions and we obtain a complete understanding of the dynamics of elements. In particular we are able to give simple proofs of several previously known results. In addition, we describe a completely dynamical solution to the conjugacy problem for one-bump functions in F , similar to the dynamical criterion for conjugacy in $PL_+(I)$ derived by Brin and Squier [19]. The material of this Chapter represents joint work with James Belk. It can also be found in [7].

3.1 Strand Diagrams

We present here a new interpretation of strand diagrams as stack machines. This provides a direct link between strand diagrams and piecewise-linear functions, and paves the way for a dynamical understanding of conjugacy. This description was inspired by a similar description of F in [34] as an “asynchronous automata group”. We have already introduced this point of view in the proof of Theorem 2.1.2.

¹It is expected that many of the results of this Chapter can also be extended to Thompson's groups T and V and to *Generalized Thompson's groups* (see Example 4.6.2).

3.1.1 Representation of Elements

Each strand diagram represents a certain piecewise-linear homeomorphism $f: I \rightarrow I$. The strand diagram is like a computer circuit: whenever a binary number $t \in [0, 1]$ is entered into the top, the signal winds its way through the circuit and emerges from the bottom as $f(t)$ (see figure 3.1).

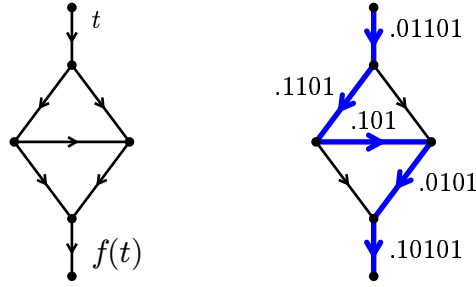


Figure 3.1: A strand diagram as a circuit

During the computation, the binary number changes each time that the signal passes through a vertex. For a split, the signal travels either left or right based on the first digit of the number (figure 3.2). The first digit is lost after the signal

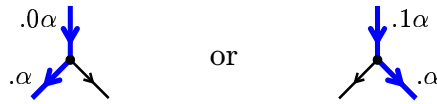


Figure 3.2: Split rule

passes through the split. For a merge, the number gains an initial 0 or a 1, depending on whether it enters from the left or from the right (figure 3.3). This describes the action of a strand diagram on the unit interval. We will show in the next section that every strand diagram acts as an element of F .

Example 3.1.1. The following figure shows the three different paths that numbers might take through a certain strand diagram:

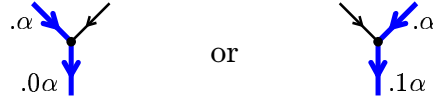


Figure 3.3: Merge rule

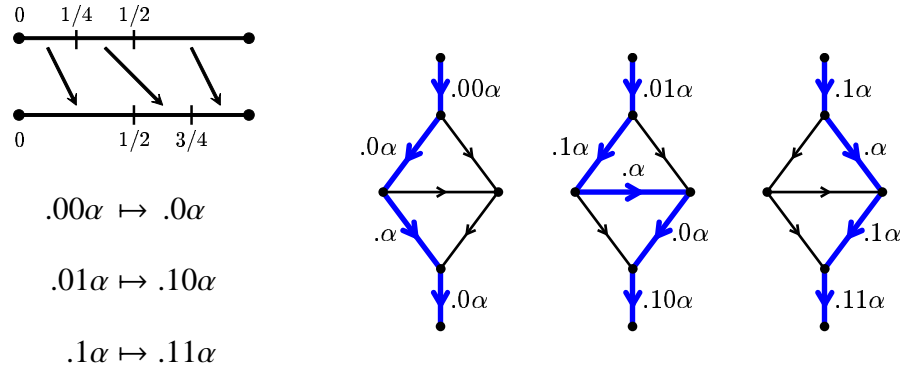


Figure: Three paths through a strand diagram

As you can see, this strand diagram acts as the element of F shown on the left.

Note 3.1.2. The scheme above is really the description of a *stack machine* represented by a strand diagram. A stack machine is similar to a finite-state automaton, except that the input and output are replaced by one or more stacks of symbols. Each state of a stack machine is either a *read state*, *write state*, or a *halt state*. A read state pops a symbol from a stack, and then moves to another state determined by which symbol was read. A write state pushes a symbol onto a stack and then moves to a specified other state. The process ends when the machine moves to a halt state. A strand diagram can be interpreted as a stack machine with one stack. Each edge represents a state of the stack machine. Edges that end with a split are read states, edges that end with a merge are write states, and the edge that ends with the sink is a halt state.

3.1.2 Reductions

Recall that a *reduction* of a strand diagram is either of the following moves:

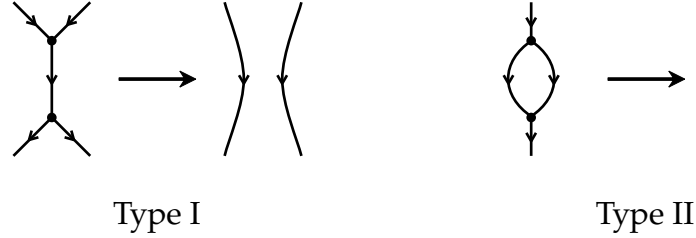


Figure: Reductions for strand diagrams

Neither of these simplifications changes the action of the strand diagram on binary sequences (see figure 3.4).

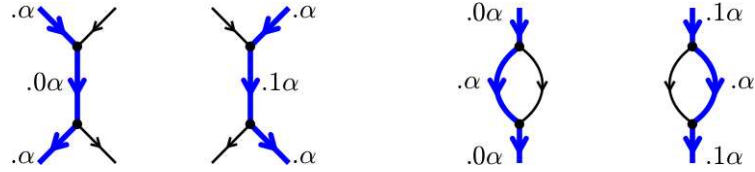


Figure 3.4: Reductions do not change the underlying map

3.1.3 (m, n) -Strand Diagrams

We look at the groupoid of (m, n) -Strand Diagrams from the dynamical point of view (see figure 3.5). Recall that a strand diagram with m sources and n sinks is called an (m, n) -strand diagram. Such a strand diagram can receive input along any of its sources; the signal then travels through the diagram according to the rules in section 3.1.1, eventually emerging from one of the sinks.

We can interpret an (m, n) -strand diagram as a piecewise-linear homeomorphism $[0, m] \rightarrow [0, n]$. Specifically, a number of the form $k + 0.\alpha$ corresponds to

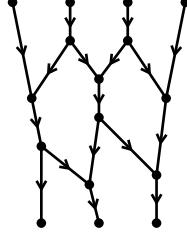


Figure 3.5: An element of Thompson's groupoid

an input of α entered into the k th source, or an output of α emerging from the k th sink. The set of piecewise-linear functions determined in this way is precisely the set of dyadic rearrangements from $[0, m]$ to $[0, n]$, i.e. the orientation-preserving homeomorphisms $[0, m] \rightarrow [0, n]$ whose slopes are powers of two, and whose breakpoints have dyadic rational coordinates.

The set of homeomorphisms described above is closed under compositions and inverses, and therefore forms a *groupoid* with objects $\{[0, 1], [0, 2], [0, 3], \dots\}$. Indeed two homeomorphisms $f : [0, m] \rightarrow [0, m]$ and $g : [0, n] \rightarrow [0, n]$ from Thompson's groupoid are conjugate if and only if they have the same reduced annular strand diagram, by the results of Chapter 2.

It is immediate to generalize this description to the case of cylindrical (m, n) -Strand Diagrams and hence to give a proof to Proposition 2.2.12.

Proposition 3.1.3 (Ghys-Sergiescu, [31]). *Every element of T has a periodic point.*

Proof. Let f be a $(1, 1)$ -cylindrical strand diagram. Up to conjugacy, we can select a reduced (k, k) -cylindrical strand diagram representing an element g conjugate to f , with k as above. We consider the toral strand diagram associated to g . Every toral strand diagram has a merge cycle λ , which thus intersects the cutting

line σ in at least one point p . This point must thus correspond to one of the k -sources of g , say the i -th source.

Since the point p lies on a merge cycle, there must be a power g^r such that the strand leaving the i -th source of g^r ends into the i -th sink. By using the right vine, we know that the i -th source corresponds to some dyadic subinterval $[a, b]$ of $[0, 1]$. Thus g^r is a continuous map that sends $[a, b]$ into itself, thus g^r must have a fixed point and so g has a periodic point. \square

3.2 Dynamics of Annular Strand Diagrams

3.2.1 Fixed points and “chaos”

In this section we survey some known results on dynamics in F . Figure 3.6 is the graph for an element of F . The main dynamical features of this element are

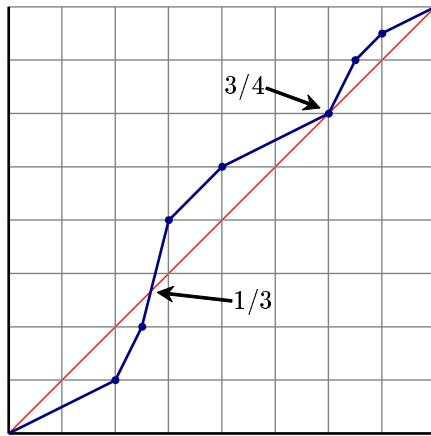


Figure 3.6: An example of an element of F

the four fixed points at 0 , $\frac{1}{3}$, $\frac{3}{4}$, and 1 . Every element of F fixes 0 and 1 , but not

every element has *interior fixed points* like $\frac{1}{3}$ and $\frac{3}{4}$. We are going to observe the properties of the fixed points of this element by studying the *local replacement rule*: we look at a one-sided neighborhood U_p of a fixed point p that is small enough so that the map $x \rightarrow f(x)$ is linear for any $x \in U_p$ and hence, if x is written in binary expansion, then $f(x)$ is obtained by adding some digits in front of x or subtracting some of the first digits of x , with the tail of the binary expansion of x and $f(x)$ remaining the same.

1. The fixed point at 0 is attracting, since the slope is $\frac{1}{2}$. The local replacement rule is $.x \mapsto .0x$, which causes points near zero to converge to zero:

$$.x \mapsto .0x \mapsto .00x \mapsto .000x \mapsto \dots$$

2. Fixed points do not have to be dyadic. In fact, the fixed point at $\frac{1}{3}$ is not a dyadic fraction. In binary, the local replacement rule is $.10x \mapsto .x$, with a fixed point at $.101010\dots = \frac{1}{3}$. The slope here is 4, so the fixed point is repelling:

$$.101010x \mapsto .1010x \mapsto .10x \mapsto .x \mapsto \dots$$

3. The fixed point at $\frac{3}{4}$ is dyadic, and has two local replacement rules: $.10x \mapsto .101x$ on the left, and $.1100x \mapsto .110x$ on the right. This makes $\frac{3}{4} = .101111\dots = .110000\dots$ attracting from the left:

$$.10x \mapsto .101x \mapsto .1011x \mapsto .10111x \mapsto \dots$$

and repelling from the right:

$$.110000x \mapsto .11000x \mapsto .1100x \mapsto .110x \mapsto \dots$$

Only an interior dyadic fixed point can have different behavior from the left and from the right, because only a dyadic rational can be a breakpoint for an element of F .

If we think of F as acting on the Cantor set, then $\frac{3}{4}$ corresponds to *two* fixed points of f : one at .101111 and the other at .110000. Each of these fixed points has a well-defined slope.

4. The fixed point at 1 is attracting, with local replacement rule $\alpha \mapsto .1\alpha$.

If we think of F as acting on the Cantor set, then each fixed point of an element of F has a well-defined slope, because dyadic rational fixed points are counted twice (as they can have different slopes on the right and on the left). The possible values of this slope depend on the tail of the fixed point:

Proposition 3.2.1. *Suppose that $f \in F$ has a fixed point at t , and let n be the eventual period of the binary expansion for t . Then the slope of f on each side of t is an integer power of 2^n . If t is non-dyadic, the slopes at the two sides must be equal.*

Proof. By hypothesis, $t = .\mu\bar{\rho}$, where ρ is a binary sequence of length n . If μ is as short as possible, then any element of F with a fixed point at t must have the local replacement rule

$$.\mu\rho^k\alpha \mapsto .\mu\alpha \quad \text{or} \quad .\mu\alpha \mapsto .\mu\rho^k\alpha$$

near t , for some $k \geq 0$. The first case gives a slope of $(2^n)^k$, and the second a slope of $(2^n)^{-k}$. \square

For example, any element of F that fixes $1/3$ must have slope 4^n at the fixed point. Because a dyadic rational has eventual period 1, the left and right slopes at a dyadic fixed point can be any powers of 2.

Most of the properties of the fixed points are preserved under conjugation:

Proposition 3.2.2. *Let $f, g \in F$, and suppose that f has fixed points at*

$$0 = t_0 < t_1 < \cdots < t_n = 1.$$

Then gfg^{-1} has fixed points at

$$0 = g(t_0) < g(t_1) < \cdots < g(t_n) = 1.$$

Moreover, the slopes of gfg^{-1} on the left and on the right of $g(t_i)$ are the same as the slopes of f on the left and on the right of t_i .

Proof. This is very elementary. The statement about slopes follows from the chain rule. \square

Thus it makes sense to talk about the “number of fixed points” for a conjugacy class of F , as well as the “slope at the 5th fixed point”. The following proposition lets us talk about the “tail of a fixed point”:

Proposition 3.2.3. *Let $t, u \in (0, 1)$. Then t and u are in the same orbit of F if and only if t and u have binary expansions with the same tail—that is, if and only if*

$$t = .\mu\omega \quad \text{and} \quad u = .v\omega$$

for some finite binary sequences μ, v and some infinite binary sequence ω .²

Proof. For the forward direction, observe that any replacement rule preserves the tail of a binary sequence. For the backwards direction, it is easy to draw a “pipeline” that implements the rule $.\mu\alpha \mapsto .v\alpha$ (see figure 3.7).

²This result cannot be extended to generalized Thompson’s groups (see Example 4.6.2). In fact, while Thompson’s group F is transitive on all dyadic rational points, this is not true anymore for generalized Thompson’s groups and n -adic rational points: we will see in Chapter 4, Remark 4.4.9.

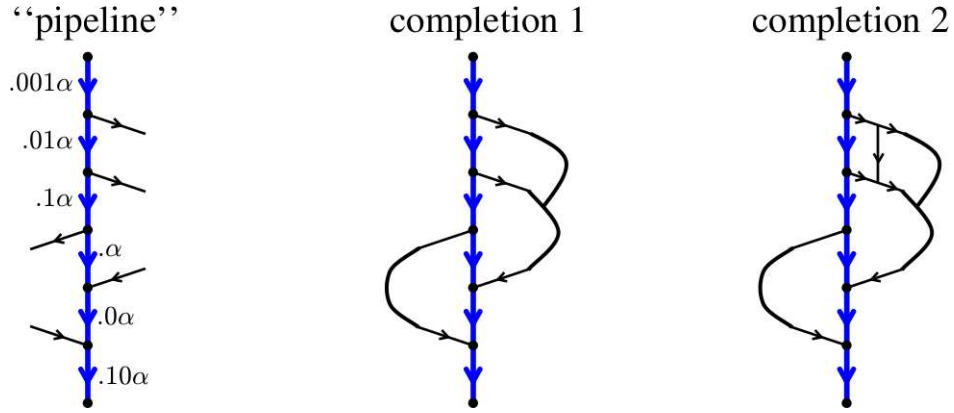


Figure 3.7: Completing an element out of a “pipeline”

Up to taking the common tail to start from a further digit, we can assume μ and ν each have both 0's and 1's (i.e. both left and right connections), otherwise $.\mu\alpha$ or $.\nu\alpha$ is 0 or 1. This drawing can easily be extended to a complete strand diagram by adding strands on the left and on the right so that all the outgoing strands can be suitably arranged to get into the ingoing ones. Figure 3.7 shows two possible ways to complete the pipeline, leading to two distinct elements of F . \square

For example, the image of $\frac{3}{4}$ under an element $g \in F$ can be any dyadic fraction, and the image of $\frac{1}{3}$ can be any rational number whose binary expansion ends in 010101... (i.e. any number whose difference from $\frac{1}{3}$ is dyadic). The previous result can be obtained using the language of piecewise-linear homeomorphisms and we will do so in Chapter 4 to get similar results (see Lemma 4.1.5 and Proposition 4.1.6).

The following proposition shows that there are no further constraints on the positions of the fixed points within a conjugacy class:

Proposition 3.2.4. *Let $0 = t_0 < \dots < t_n = 1$ and $0 = u_0 < \dots < u_n = 1$, and suppose that each t_i is in the same F -orbit as the corresponding u_i . Then there exists an*

element of F that maps (t_0, \dots, t_n) to (u_0, \dots, u_n) .

Sketch of the Proof. A strand diagram for the required element can be constructed using a method similar to the proof of the previous proposition. See Corollary 4.1.8 for another proof using different techniques. \square

3.2.2 Cut Paths and Thompson's Groupoid

Thompson's groupoid is fundamental to the study of conjugacy in F . For example, figure 3.8 shows three strand diagrams that represent conjugate elements of F . Each of these elements begins by partitioning $[0, 1]$ into four subintervals,

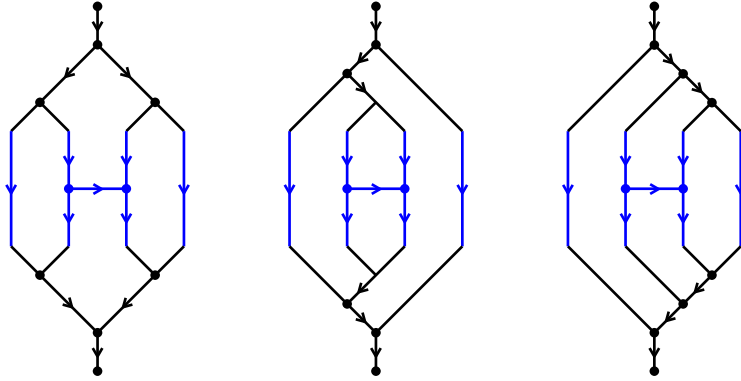


Figure 3.8: Three conjugate elements

and ends by recombining these four subintervals into $[0, 1]$. They differ only in the choice of the partition. These elements are all conjugate to the element of Thompson's groupoid shown in figure 3.9. As you can see, this homeomorphism $[0, 4] \rightarrow [0, 4]$ is simpler than any of the elements of F above. Indeed, this element is a *minimal* representative for its conjugacy class, in the sense that it is reduced (it has the fewest possible splits and merges). The reason is that any

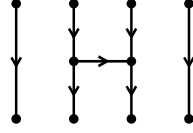


Figure 3.9: A minimal representative

element of this conjugacy class must have at least as many splits and merges as the reduced annular strand diagram of figure 3.10.

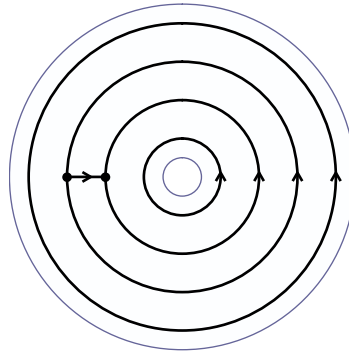


Figure 3.10: The corresponding reduced annular strand diagram

By Propositions 2.1.8 and 2.1.10 we know that any two cut paths of an annular strand diagrams yield conjugate elements. Hence, minimal representatives of a conjugacy class are precisely those obtained by cutting the reduced annular strand diagram along some cut path.

3.2.3 Directed Loops and Fixed Points

It is possible for an element of F to have infinitely many fixed points. For example, the identity element fixes the entire interval $[0, 1]$, and any element of F can have a linear segment that coincides with the identity on some interval $[d, e]$ (d and e dyadic). If $f \in F$, a *fixed interval* of f is either

1. An isolated fixed point $\{t\}$ of f , or
2. A maximal open interval of fixed points,
3. An endpoint of a maximal open interval of fixed points.

Convention 3.2.5. Each isolated interior dyadic fixed point of f corresponds to two fixed intervals.

Theorem 3.2.6. *Let $f \in F$, and let S be the reduced annular strand diagram for f . Then the directed loops L_0, \dots, L_n of S (ordered from outside to inside) are in one-to-one correspondence with the fixed intervals $I_0 < \dots < I_n$ of f . This correspondence has the following properties:*

1. *Every free loop corresponds to a maximal interval of fixed points.*
2. *Every split loop corresponds to an isolated repeller. In particular, a split loop with n splits corresponds to a fixed point with slope 2^n .*
3. *Every merge loop corresponds to an isolated attractor. In particular, a merge loop with n merges corresponds to a fixed point with slope 2^{-n} .*

In the latter two cases, the pattern of outward and inward connections around the loop determines the tail of the binary expansion of the fixed point. Specifically, each outward connection corresponds to a 1, and each inward connection corresponds to a 0.

Remark 3.2.7. The previous result induces an order on the components and the directed cycles for annular strand diagrams, going from the inside to the outside. Compare this result with part 5 of Proposition 2.1.13.

Proof. We have already shown that all of the information outlined in the statement of the theorem is conjugacy invariant. Therefore, we may replace f by

any element whose reduced annular strand diagram is S . Specifically, we may assume that f is the dyadic rearrangement $[0, k] \rightarrow [0, k]$ obtained by cutting S along a cutting path c .

S contains a merge loop: some of the vertices on this loop are coming from the inner part of the loop, while some are coming from the outer part of the loop. We work out an example in detail. The general procedure follows closely from it, as it will become apparent that the general case does not depend on the number of vertices on the loops. Suppose that S contains the merge loop in figure 3.11. The cutting path c cuts through this loop exactly once, along

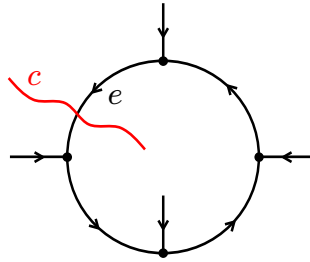


Figure 3.11: An example of a merge loop

some edge e . If we place a binary number β along e , the number will trace a directed path through the annular strand diagram, changing in value every time it passes through a vertex. Assuming that c crosses i edges before crossing e , this corresponds to feeding $i + \beta$ into the strand diagram for f .

In the case we are considering, the number will simply travel around the merge loop (see figure 3.12). By the time it returns to e , its value will be the fractional part of $f(i + \beta)$. If we continue following the number along the merge loop, the values it has when it passes through e will be the fractional parts of the iterates $f^n(i + \beta)$. In the case that we are considering, it follows that:

$$f(i + \beta) = i + .1101\beta \quad f^2(i + \beta) = i + .1101\,1101\beta \quad \text{etc.}$$

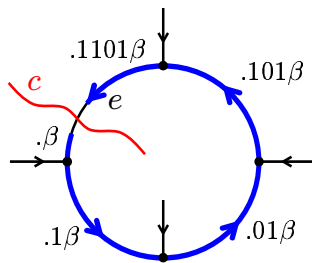


Figure 3.12: Traveling through the merge loop

In particular, the number $\alpha = i + .\overline{1101}$ is a fixed point of f .

Note that the sequence 1101 is determined by the counterclockwise pattern of inward and outward edges, exactly as stated in the theorem. In addition, we have shown that f is linear on $[i, i + 1]$, with formula:

$$f(i + .\beta) = i + .1101\beta$$

This linear function has slope 2^{-4} . This implies that α is an attracting fixed point—indeed, for any $i + .\beta \in [i, i + 1]$, the first $4n$ digits of $f^n(i + .\beta)$ are the same as the first $4n$ digits of α .

A split loop works in roughly the same way, except that a split loop is repelling (see figure 3.13). Note that every fixed point of f arises from either a

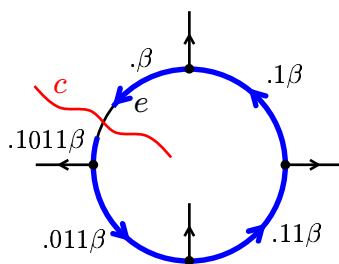


Figure 3.13: An example of a split loop

split loop or merge loop. In particular, suppose that $i + .\beta$ is a fixed point of f ,

and let e be the $(i + 1)$ 'st edge crossed by c . If we place the binary number β along e , then the resulting path of motion must wind once around the central hole and then return to e with value β . It follows that β must have traveled around a directed loop, and $i + \beta$ is the unique fixed point determined by the loop. \square

Note that the outermost loop of an annular strand diagram for $f \in F$ corresponds to the fixed point $0 = .0000 \dots$, while the innermost loop corresponds to the fixed point $1 = .1111 \dots$. Within each connected component of S , the outermost and innermost loops correspond to dyadic fixed points, while the interior loops correspond to non-dyadic fixed points.

Corollary 3.2.8. *Let S be the reduced annular strand diagram for an element $f \in F$. Then every component of S corresponds to exactly one of the following:*

1. *A maximal open interval of fixed points of f (for a free loop), or*
2. *A maximal interval with no dyadic fixed points of f in its interior.*

If $f \in F$, a *cut point* of f is either an isolated dyadic fixed point of f , or an endpoint of a maximal interval of fixed points. If $0 = \alpha_0 < \alpha_1 < \dots < \alpha_n = 1$ are the cut points of f , then the restrictions $f_i: [\alpha_{i-1}, \alpha_i] \rightarrow [\alpha_{i-1}, \alpha_i]$ are called the *components* of f (see figure 3.14). Each component of f corresponds to one connected component of the reduced annular strand diagram (figure 3.15). We recall if $\alpha < \beta$ are any dyadic rationals, there exists a Thompson-like homeomorphism $\varphi: [\alpha, \beta] \rightarrow [0, 1]$ such that any map in $\text{PL}_2([\alpha, \beta])$ can be conjugated by φ to become an element of F by Corollary 1.1.6.

Proposition 3.2.9. *Let $f \in F$ have components $f_i: [\alpha_{i-1}, \alpha_i] \rightarrow [\alpha_{i-1}, \alpha_i]$, and let S be the reduced annular strand diagram for f . Then for each i , the component of*

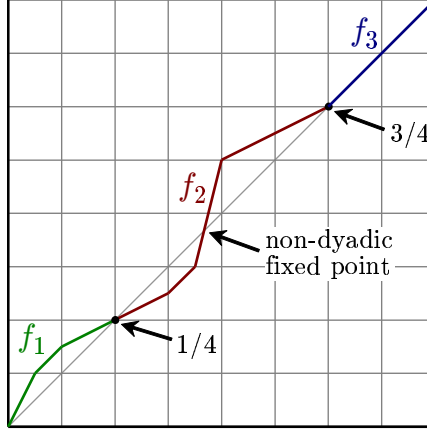


Figure 3.14: Components of a function

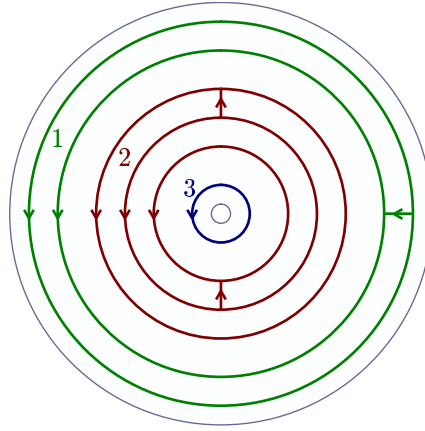


Figure 3.15: Annular strand diagram for a component

S corresponding to f_i is the reduced annular strand diagram for any element of F conjugate to f_i .

Proof. Suppose f has $n + 1$ cut points $0 = \alpha_0 < \alpha_1 < \dots < \alpha_n = 1$. Then we can conjugate f to an element of Thompson's groupoid whose cut points are at $0, 1, 2, \dots, n$. The resulting (n, n) -strand diagram has n connected components which, when reduced, yield the n components of S . \square

Corollary 3.2.10. Let $f, g \in F$ have components f_1, \dots, f_n and g_1, \dots, g_n . Then f is conjugate to g in F if and only if each f_i is conjugate to g_i through some

Thompson-like homeomorphism.

3.3 Mather Invariants

Conjugacy in F was first investigated by Brin and Squier [19], who successfully found a criterion for conjugacy in the full group of piecewise-linear homeomorphisms of the interval. This solution was based on some ideas of Mather [48] for determining whether two given diffeomorphisms of the unit interval are conjugate.

In this section we show that solution we have proved in Chapter 2 can be described in a way similar to the solutions given by Mather for $\text{Diff}_+(I)$ and by Brin and Squier for $\text{PL}_+(I)$. Specifically, we define a Mather-type invariant for elements of F , and show that two one-bump functions in F are conjugate if and only if they have the same Mather invariant.

A somewhat different dynamical description of conjugacy in F has been obtained independently by Gill and Short [32].

3.3.1 Background on Mather Invariants

Consider the group $\text{Diff}_+(I)$ of all orientation-preserving diffeomorphisms of $[0, 1]$.

Definition 3.3.1. A *one-bump function* is an element $f \in \text{Homeo}_+(I)$ such that $f(x) > x$ for all $x \in (0, 1)$.

Figure 3.16 shows an example of a one-bump function. By the chain rule,

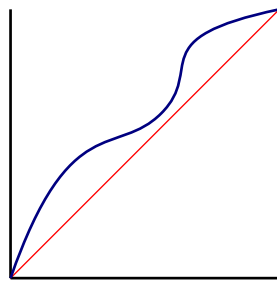


Figure 3.16: A one-bump function

two one-bump functions $f, g \in \text{Diff}_+(I)$ can only be conjugate if $f'(0) = g'(0)$ and $f'(1) = g'(1)$, but this condition is not sufficient. In 1973, Mather constructed a more subtle conjugacy invariant of one-bump functions f such that $f'(0) > 1$ and $f'(1) < 1$, and proved that two such one-bump functions in $\text{Diff}_+(I)$ are conjugate if and only if they have the same slopes at 0 and 1 and the same Mather invariant. In 1995, Yoccoz extended this to a complete criterion for conjugacy in $\text{Diff}_+(I)$ [62]. Similar invariants are used for conjugacy of diffeomorphisms in [3], [63], and [1], the last of which introduces the term “Mather invariant”.

In 2001 [19], Brin and Squier³ extended Mather’s analysis to the group $\text{PL}_+(I)$ of all orientation-preserving piecewise-linear homeomorphisms of $[0, 1]$. Specifically, they defined a Mather invariant for one-bump functions in $\text{PL}_+(I)$, and showed that two one-bump functions are conjugate if and only if they have the same slopes at 0 and 1 and the same Mather invariant. Using this result, they went on to describe a complete criterion for conjugacy in $\text{PL}_+(I)$.

The Mather invariant is simpler to describe in the piecewise-linear case. The following description is based on the geometric viewpoint introduced in [63] and [1], so the language differs considerably from that used in [19] or [48].

³Brin and Squier originally developed this theory in 1987, but it was published in 2001.

Consider a one-bump function $f \in \text{PL}_+(I)$, with slope m_0 at 0 and slope m_1 at 1. In a neighborhood of zero, f acts as multiplication by m_0 ; in particular, for any sufficiently small $t > 0$, the interval $[t, m_0 t]$ is a fundamental domain for the action of f (see figure 3.17). If we make the identification $t \sim m_0 t$ in the interval

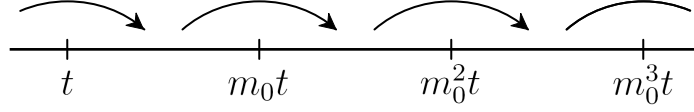


Figure 3.17: Action of f in a neighborhood of 0

$(0, \epsilon)$, we obtain a circle C_0 , with partial covering map $p_0: (0, \epsilon) \rightarrow C_0$. Note that the restriction of f is a deck transformation of this cover:

$$\begin{array}{ccc} (0, \epsilon) & \xrightarrow{f} & (0, \epsilon) \\ & \searrow p_0 & \swarrow p_0 \\ & C_0 & \end{array}$$

Similarly, if we identify $(1 - t) \sim (1 - m_1 t)$ on the interval $(1 - \delta, 1)$, we obtain a circle C_1 , with partial covering map $p_1: (1 - \delta, 1) \rightarrow C_1$.

If N is sufficiently large, then f^N will take some lift of C_0 to $(0, \epsilon)$ and map it to the interval $(1 - \delta, 1)$. This induces a map $f^\infty: C_0 \rightarrow C_1$, making the following diagram commute:

$$\begin{array}{ccc} (0, \epsilon) & \xrightarrow{f^N} & (1 - \delta, 1) \\ p_0 \downarrow & & \downarrow p_1 \\ C_0 & \xrightarrow{f^\infty} & C_1 \end{array}$$

Definition 3.3.2. The map f^∞ defined above is the Mather invariant for f .

We note that f^∞ does not depend on the specific value of N chosen. Any map f^m , for $m \geq N$, induces the same map f^∞ . This is because f acts as the identity on

C_1 by construction and f^m can be written as $f^{m-N}(f^N(t))$, with $f^N(t) \in (1 - \delta, 1)$. If $k > 0$, then the map $t \mapsto kt$ on $(0, \epsilon)$ induces a “rotation” rot_k of C_0 . In particular, if we use the coordinate $\theta = \log t$ on C_0 , then

$$\text{rot}_k(\theta) = \theta + \log k$$

so rot_k is an actual rotation.

Theorem 3.3.3 (Brin and Squier). *Let $f, g \in \text{PL}_+(I)$ be one-bump functions with $f'(0) = g'(0) = m_0$ and $f'(1) = g'(1) = m_1$, and let $f^\infty, g^\infty: C_0 \rightarrow C_1$ be the corresponding Mather invariants. Then f and g are conjugate if and only if f^∞ and g^∞ differ by rotations of the domain and range circles:*

$$\begin{array}{ccc} C_0 & \xrightarrow{f^\infty} & C_1 \\ \text{rot}_k \downarrow & & \downarrow \text{rot}_\ell \\ C_0 & \xrightarrow{g^\infty} & C_1 \end{array}$$

Proof. We will show here that conjugate elements have similar Mather invariants. See [19] for the converse.

Suppose that $f = h^{-1}gh$ for some $h \in \text{PL}_+(I)$. Then the following diagram commutes, where $k = h'(0)$ and $\ell = h'(1)$:

$$\begin{array}{ccccc} & & (0, \epsilon) & \xrightarrow{g^N} & (1 - \delta, 1) \\ & \nearrow h & \downarrow & & \nearrow h \\ (0, \epsilon) & \xrightarrow{f^N} & (1 - \delta, 1) & & \\ \downarrow p_0 & & \downarrow p_0 & & \downarrow p_1 \\ & & C_0 & \xrightarrow{g^\infty} & C_1 \\ \downarrow p_0 & \nearrow \text{rot}_k & & & \nearrow \text{rot}_\ell \\ C_0 & \xrightarrow{f^\infty} & C_1 & & \end{array} \quad \square$$

For diffeomorphisms, one-bump functions are not linear in neighborhoods of 0 and 1, but it is still possible to define the Mather invariant by taking a limit as $t \rightarrow 0$ and $t \rightarrow 1$. (Essentially, a one-bump function in $\text{Diff}_+(I)$ acts linearly on infinitesimal neighborhoods of 0 and 1.) In this case, the Mather invariant is a C^∞ function $C_0 \rightarrow C_1$.

Theorem 3.3.4 (Mather, Young). *Two one-bump functions $f, g \in \text{Diff}_+(It)$ with the same slopes at 0 and 1 are conjugate if and only if f^∞ and g^∞ differ by rotations of the domain and range.*

We conclude this section by remarking that Mather invariants have been defined for diffeomorphisms acting on higher dimensional manifolds. In [1], Afraimovich and Young extend this result to a certain class of diffeomorphisms of the sphere S^2 . Specifically, they consider diffeomorphisms f of the sphere with two fixed points, one a hyperbolic attractor and the other a hyperbolic repeller, with the property that all of the orbits are heteroclinic from the repeller to the attractor. By choosing fundamental annuli for Df in the tangent spaces of the two fixed points, one can construct a Mather invariant for such diffeomorphisms which is a smooth map between two tori.

3.3.2 Mather Invariants for F

In this section, we show that the reduced annular strand diagram for a one-bump function in F can be interpreted as a Mather invariant. Therefore, two one-bump functions in F are conjugate in F if and only if they have the same Mather invariant. We also briefly describe the dynamical meaning of reduced annular strand diagrams for more complicated elements, thereby giving a com-

pletely dynamical description for conjugacy in F .

Definition 3.3.5. The *piecewise-linear logarithm* $\text{PLog}: (0, \infty) \rightarrow (-\infty, \infty)$ is the piecewise-linear function that maps the interval $[2^k, 2^{k+1}]$ linearly onto $[k, k+1]$ for every $k \in \mathbb{Z}$ (see figure 3.18).

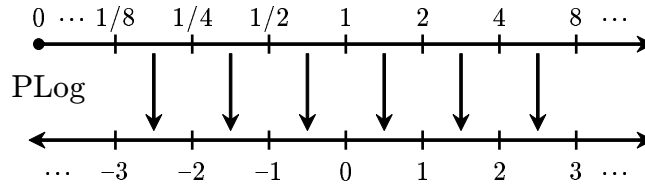


Figure 3.18: The PLog map

Suppose that $f \in F$ is a one-bump function with slope 2^m at 0 and slope 2^{-n} at 1, and let $f^\infty: C_0 \rightarrow C_1$ be the corresponding Mather invariant. In a neighborhood of 0, the function f acts as multiplication by 2^m . In particular, $\text{PLog } f(t) = m + \text{PLog } t$ for all $t \in (0, \epsilon)$, so we can identify C_0 with the circle $\mathbb{R}/m\mathbb{Z}$. Figure 3.19 shows the case $m = 3$: In a similar way, we can use the func-

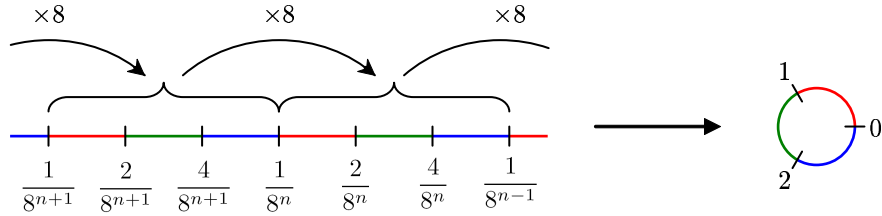


Figure 3.19: Construction of the circle C_0

tion $t \mapsto -\text{PLog}(1 - t)$ to identify C_1 with the circle $\mathbb{R}/n\mathbb{Z}$. This lets us regard the Mather invariant for f as a function $f^\infty: \mathbb{R}/m\mathbb{Z} \rightarrow \mathbb{R}/n\mathbb{Z}$. Because f^N and PLog are piecewise-linear, the Mather invariant f^∞ is a piecewise-linear function. Moreover, f^∞ is Thompson-like: all the slopes are powers of 2, and the breakpoints are dyadic rational numbers of $\mathbb{R}/m\mathbb{Z} = [0, m]/\{0, m\}$.

Now, if $k \in \mathbb{Z}$, then the map $t \mapsto 2^k t$ on $(0, \epsilon)$ induces a "rotation" of C_0 . Using our new scheme, this is precisely an integer rotation of $\mathbb{R}/m\mathbb{Z}$:

$$\text{rot}_k(\theta) = \theta + k \pmod{m}$$

We are now ready to state the main theorem:

Theorem 3.3.6. *Let $f, g \in F$ be one-bump functions with $f'(0) = g'(0) = 2^m$ and $f'(1) = g'(1) = 2^{-n}$, and let $f^\infty, g^\infty: \mathbb{R}/m\mathbb{Z} \rightarrow \mathbb{R}/n\mathbb{Z}$ be the corresponding Mather invariants. Then f and g are conjugate if and only if f^∞ and g^∞ differ by integer rotations of the domain and range circles:*

$$\begin{array}{ccc} \mathbb{R}/m\mathbb{Z} & \xrightarrow{f^\infty} & \mathbb{R}/n\mathbb{Z} \\ \text{rot}_k \downarrow & & \downarrow \text{rot}_\ell \\ \mathbb{R}/m\mathbb{Z} & \xrightarrow{g^\infty} & \mathbb{R}/n\mathbb{Z} \end{array}$$

The forward direction follows from the same argument given for proposition 3.3.3. The converse is more difficult: we must show that any two one-bump functions whose Mather invariants differ by integer rotation are conjugate in F . To prove this, we describe an explicit correspondence between Mather invariants and reduced annular strand diagrams.

If $f \in F$ is a one-bump function, then the only fixed points of f are at 0 and 1. Therefore, the reduced annular strand diagram for f has only two directed cycles (see figure 3.20). Since $f'(0) > 1$, the outer cycle (corresponding to 0) must be a split loop, and the inner cycle (corresponding to 1) must be a merge loop. If we remove these two cycles, we get an (m, n) -strand diagram drawn on a cylinder (see figure 3.21). In Chapter 2, this is referred to as a *cylindrical strand diagram*. Such a diagram can be used to describe a Thompson-like map between two circles.

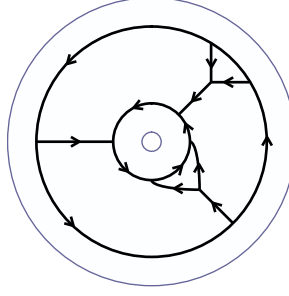


Figure 3.20: Annular strand diagram for a one-bump function

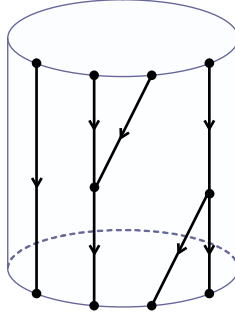


Figure 3.21: From an annular strand diagram to a cylindrical one

Proposition 3.3.7. *There is a one-to-one correspondence between*

1. *Reduced cylindrical (m, n) -strand diagrams, and*
2. *Thompson-like functions $\mathbb{R}/m\mathbb{Z} \rightarrow \mathbb{R}/n\mathbb{Z}$, with two functions considered equivalent if they differ by integer rotation of the domain and range circles.*

Proof. A *labeling* of a cylindrical (m, n) strand diagram is a counterclockwise assignment of the numbers $1, 2, \dots, m$ to the sources, and a counterclockwise assignment of the numbers $1, 2, \dots, n$ to the sinks (see figure 3.22). Given a labeling, we can interpret the cylindrical strand diagram as a function $\mathbb{R}/m\mathbb{Z} \rightarrow \mathbb{R}/n\mathbb{Z}$, with the source labeled k corresponding to the interval $[k - 1, k] \subset \mathbb{R}/\mathbb{Z}$, and so forth. We claim that labeled reduced cylindrical (m, n) -strand diagrams are in

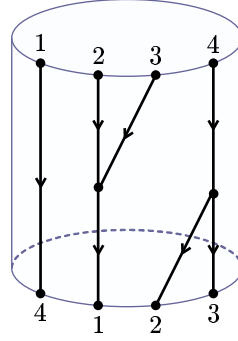


Figure 3.22: Labeling of a cylindrical strand diagram

one-to-one correspondence with Thompson-like functions $\mathbb{R}/m\mathbb{Z} \rightarrow \mathbb{R}/n\mathbb{Z}$.

The argument is similar to the proof of Theorem 2.1.2. Suppose we are given a Thompson-like homeomorphism $f: \mathbb{R}/m\mathbb{Z} \rightarrow \mathbb{R}/n\mathbb{Z}$ (see figure 3.23). Then

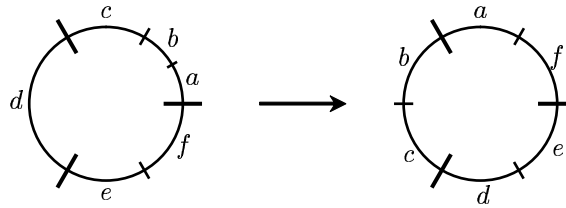


Figure 3.23: A circle map

we can construct a pair of binary forests representing the dyadic subdivisions of the domain and range circles (see figure 3.24). The forest for the domain has

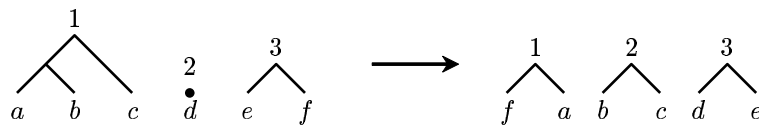


Figure 3.24: A forest diagram for the circle map

m trees (corresponding to the subdivisions of the intervals $[0, 1], [1, 2], \dots, [m - 1, m]$ in $\mathbb{R}/m\mathbb{Z}$), and the forest for the range has n trees. Since the function f is continuous, it must preserve the cyclic order of the intervals. Therefore, we can

construct a strand diagram for f by attaching the leaves of the top forest to the leaves of the bottom forest via some cyclic permutation (see figure 3.25). This

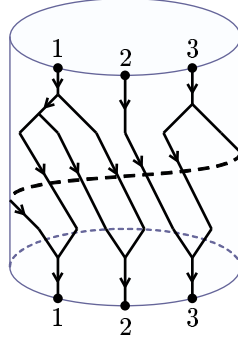


Figure 3.25: The constructed labeled cylindrical strand diagram

gives a labeled cylindrical strand diagram for f . Conversely, given any reduced labeled cylindrical (m, n) -strand diagram, we can cut along every edge that goes from a split to a merge. This decomposes the cylindrical strand diagram into two forests, and therefore specifies a Thompson-like homeomorphism f .

Finally, note that changing the labeling of the sources of a cylindrical (m, n) -strand diagram has the effect of performing an integer rotation on the domain of the corresponding function. Similarly, changing the labeling of the sinks performs an integer rotation on the range. \square

All that remains is the following:

Proposition 3.3.8. *Let \mathcal{A} be the reduced annular strand diagram for a one-bump function $f \in F$, and let C be the cylindrical (m, n) -strand diagram obtained by removing the merge and split loops from \mathcal{A} . Then C is the cylindrical strand diagram for the Mather invariant $f^\infty: \mathbb{R}/m\mathbb{Z} \rightarrow \mathbb{R}/n\mathbb{Z}$.*

Proof. Let $f: [0, k] \rightarrow [0, k]$ be the one-bump function obtained by cutting a

reduced annular strand diagram \mathcal{A} along a cutting path c . Let e_0 and e_1 be the edges on the inner and outer loops crossed by c .

If we place a binary number along e_0 , it will circle the split loop for a while, eventually exiting along some edge. This edge depends on the length of the initial string of zeroes in the binary expansion of the number (figure 3.26). In

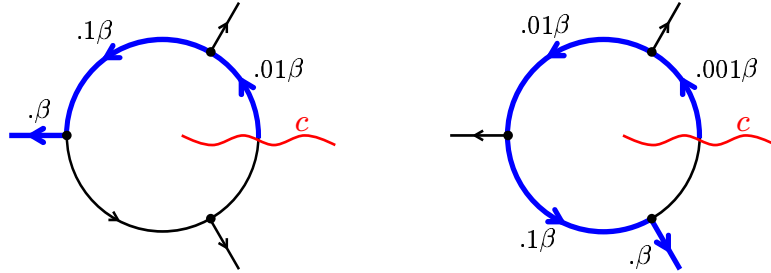


Figure 3.26: Traveling through a split loop

particular, a number leaves along the i th edge with value $.\beta$ if and only if the image of the number in $\mathbb{R}/m\mathbb{Z}$ is $(i - 1) + .\beta$.

After leaving the split loop, the number travels through the cylindrical strand diagram for the circle map, eventually entering the merge loop. If we stop the number when it reaches the edge e_1 , it will have the form $.11 \cdots 10\gamma$, where γ is the fractional part of the image of $(i - 1) + .\beta$ under the circle map, and the length of the string of 1's determines the integer part. \square

This completes the proof of theorem 3.3.6.

CHAPTER 4

THE SIMULTANEOUS CONJUGACY PROBLEM IN GROUPS OF PIECEWISE LINEAR FUNCTIONS

In this chapter we look at Thompson's group F as a group of piecewise-linear homeomorphisms and solve the simultaneous conjugacy problem for F and suitable F -like groups of piecewise linear homeomorphisms containing F .

For a fixed $k \in \mathbb{N}$, we say that the group G has *solvable k -simultaneous conjugacy problem* if there is an algorithm such that, given any two k -tuples of elements in G , $(x_1, \dots, x_k), (y_1, \dots, y_k)$, one can determine whether there is, or not, a $g \in G$ such that $g^{-1}x_i g = y_i$ for all $i = 1, \dots, k$. We say that there is an *effective solution* if the algorithm produces such an element g , in addition to proving its existence.

This problem was studied before for various classes of groups. The k -simultaneous conjugacy problem has been proved to be solvable for the matrix groups $\mathrm{GL}_n(\mathbb{Z})$ and $\mathrm{SL}_n(\mathbb{Z})$ by Sarkisyan in 1979 in [59] and independently by Grunewald and Segal in 1980 in [35]. In 1984 Scott constructed examples of finitely presented infinite simple groups that have an unsolvable conjugacy problem in her paper [60]. In their 2005 paper [13] Bridson and Howie constructed examples of finitely presented groups where the ordinary conjugacy problem is solvable, but the k -simultaneous conjugacy problem is unsolvable for every $k \geq 2$.

We will give a solution of the k -simultaneous conjugacy problem for Thompson's group F and then generalize it to the groups $\mathrm{PL}_{S,G}(J)$ (defined in Chapter 1), for an interval J with endpoints in S . We observe that in order to make some

calculations possible inside the ring S and its quotients, we need to impose some computability requirements in S . These will be clearly stated in Remark 4.4.7 and will be assumed from then on. The material of this Chapter represents joint work with Martin Kassabov. It can also be found in [42].

4.1 The Ordinary Conjugacy Problem for $\text{PL}_2(I)$

We begin our investigation with the special case of Thompson's group F , seen as the group $\text{PL}_2(I)$. Most of the techniques that we develop for this case will extend to the general case of $\text{PL}_{S,G}(I)$.

We prove a sequence of lemmas which will yield the solution to the ordinary conjugacy problem, that is, the k -simultaneous conjugacy problem with $k = 1$. To attack the ordinary conjugacy problem, we will split the study into that of some families of functions inside $\text{PL}_2(I)$. The reduction to these subfamilies will come from the study of the fixed point subset of the interval I for a function f . For an interval $J = [\eta, \zeta] \subseteq I$, a function $f \in \text{PL}_2(J)$ can be extended to the interval I by $f(t) = t$ for $t \in I \setminus J$, which allows us to consider $\text{PL}_2(J)$ as a subgroup of $\text{PL}_2(I)$. Throughout the chapter we will assume the interval J to have dyadic endpoints, so that $\text{PL}_2(J) \cong \text{PL}_2(I)$. If one of the two endpoints is not dyadic, we define $\text{PL}_2(J)$ to be the group of restrictions of functions in $\text{PL}_2(I)$ fixing the endpoints of J , that is

$$\text{PL}_2(J) = \{f|_J \mid f \in \text{PL}_2(I), f(\eta) = \eta, f(\zeta) = \zeta\}.$$

We state the following interesting question:

Question 4.1.1. Let J be an interval such that at least one of its endpoints is non-dyadic. Is the group $\text{PL}_2(J)$ finitely generated?

For a function $f \in \text{PL}_2(J)$ we define the following closed set:

$$D_J(f) := \{t \in J \mid f(t) = t\},$$

where, to simplify the notation, we will often drop the subscript J . The motivation for introducing this subset is easily explained — If $y, z \in \text{PL}_+(J)$ are conjugate through $g \in \text{PL}_+(I)$ and $s \in (\eta, \zeta)$ is such that $y(s) = s$ then $z(g^{-1}(s)) = (g^{-1}yg)(g^{-1}(s)) = g^{-1}(s)$, that is, if y has a fixed point then z must have a fixed point. For a subset $S \subseteq J$, we denote by ∂S the usual boundary of S in J .

Definition 4.1.2. We define $\text{PL}_+^<(J)$ (respectively, $\text{PL}_+^>(J)$) to be the set of all functions in $\text{PL}_+(J)$ with graph strictly below the diagonal (respectively, above the diagonal). Similarly, we can define $\text{PL}_2^<(J)$ (respectively $\text{PL}_2^>(J)$) as the set of all functions of $\text{PL}_2(J)$ with graph strictly below the diagonal (respectively, above the diagonal).

Since $x \in \text{PL}_2(I)$ has only finitely many breakpoints, $D(x)$ consists of a disjoint union of a finite number of closed intervals and isolated points. It is easy to see that $\partial D(x) \subseteq \mathbb{Q}$. As mentioned before, if $g^{-1}yg = z$, then $D(y) = g(D(z))$. Thus, as a first step we need to know if, given y and z , there exists a $g \in \text{PL}_2(I)$ such that $D(y) = g(D(z))$ and, in particular, $\partial D(y) = g(\partial D(z))$.

Our strategy will be the following: first we will find a way to verify if we can make $\partial D(y)$ coincide with $\partial D(z)$ through conjugation. Then we reduce the problem to $\partial D(y) = \partial D(z) = \{\alpha_1, \dots, \alpha_n\}$ and so we can focus on solving the conjugacy problem on each group $\text{PL}_2([\alpha_i, \alpha_{i+1}])$. If $y = z = \text{id}$ on the interval $[\alpha_i, \alpha_{i+1}]$ there is nothing to prove, otherwise we can suppose that both y, z are below/above the diagonal on $[\alpha_i, \alpha_{i+1}]$. This case will be dealt with through a procedure called the “stair algorithm” that we provide in section 4.1.3. However, we observe that

the α_i 's described above need not be dyadic. The example in figure 4.1 shows a function with a non-dyadic rational fixed point. In order to avoid working in intervals J where the endpoints may not be dyadic, we introduce a new definition of boundary which deals with this situation: for a subset S , we define

$$\partial_2 S := \partial S \cap \mathbb{Z} \left[\frac{1}{2} \right]$$

With this definition, the set $\partial S \setminus \partial_2 S$ becomes the set of isolated non-dyadic points of S .

Definition 4.1.3. We define $\text{PL}_2^0(J) \subseteq \text{PL}_2(J)$ to be the set of functions $f \in \text{PL}_2(J)$ such that the set $D(f)$ does not contain dyadic rational points other than the endpoints of J , i.e., $D(f)$ is discrete and $\partial_2 D(f) = \partial_2 J = \partial J$.

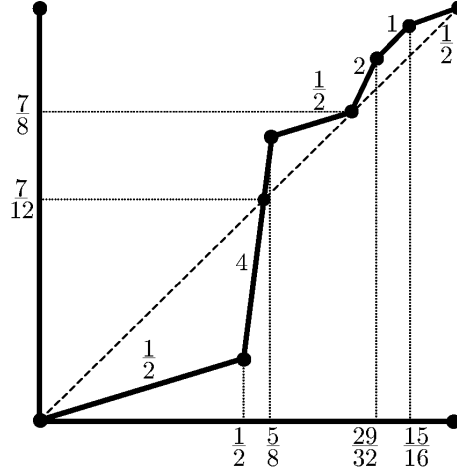


Figure 4.1: A function with a non-dyadic fixed point.

4.1.1 Making $D(y)$ and $D(z)$ coincide

Theorem 4.1.4. *Given $y, z \in \text{PL}_2(I)$, we can determine if there is (or not) a $g \in \text{PL}_2(I)$ such that $g(D(y)) = D(g^{-1}yg) = D(z)$. If such an element exists, it can be constructed.*

To start off, we need a tool to decide if this can be proved for the boundaries of the fixed point sets. In other words, we need to decide if it is possible to make $\partial D(y)$ coincide with $\partial D(z)$ (see figure 4.2). The first step is to see how, given two rational numbers α and β , we can find a $g \in \text{PL}_2(I)$ with $g(\alpha) = \beta$. The next two results are well known:

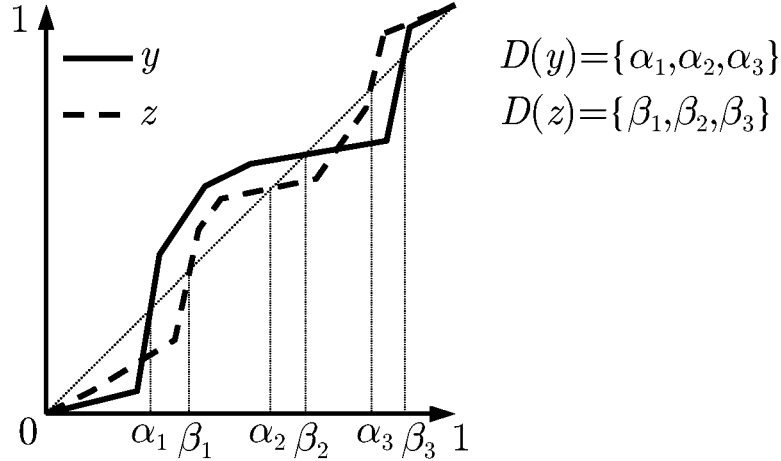


Figure 4.2: An example with $\partial D(y) \neq \partial D(z)$.

Lemma 4.1.5 (Extension of Partial Maps). *Suppose $I_1, \dots, I_k \subseteq [0, 1]$ is a family of disjoint compact intervals $I_i = [a_i, b_i]$, with $b_i < a_{i+1}$ for all $i = 1, \dots, k$ and $a_i, b_i \in \mathbb{Z}[\frac{1}{2}]$. Let $J_1, \dots, J_k \subseteq [0, 1]$, with $J_i = [c_i, d_i]$, be another family of intervals with the same property. Suppose that $g_i : I_i \rightarrow J_i$ is a piecewise-linear function with a finite number of breakpoints, occurring at dyadic rational points, and*

such that all slopes are integral powers of 2. Then there exists an $\widetilde{g} \in \text{PL}_2(I)$ such that $\widetilde{g}|_{I_i} = g_i$.

Proof. By our hypotheses we have that $0 < a_1 < b_1 < \dots < a_k < b_k < 1$ and $0 < c_1 < d_1 < \dots < c_k < d_k < 1$ are two partitions of $[0, 1]$ with the same number of points. By Lemma 1.1.4, there exists an $h \in \text{PL}_2(I)$ with $h(a_i) = c_i$ and $h(b_i) = d_i$.

Define

$$\widetilde{g}(t) := \begin{cases} h(t) & t \notin I_1 \cup \dots \cup I_k \\ g_i(t) & t \in I_i \end{cases}$$

This function satisfies the extension condition. \square

We observe that this proof is constructive and produces easily an element of F seen as a piecewise-linear function. The previous result is an analogue of the proof of Proposition 3.2.3. In fact, another way to build an extension of a partial map would be to write down the strand diagrams for the various given pieces and then fill them in between by adding strands.

Proposition 4.1.6. *Let $\alpha, \beta \in \mathbb{Q} \cap (0, 1)$. Then there is a $g \in F$ such that $g(\alpha) = \beta$ iff*

$$\alpha = \frac{2^t m}{n}, \quad \beta = \frac{2^k u}{n},$$

with $t, k \in \mathbb{Z}$, m, n, u odd integers, $(m, n) = (u, n) = 1$, and the following holds

$$u \equiv 2^R m \pmod{n} \tag{4.1}$$

for some $R \in \mathbb{Z}$.

Proof. Suppose that there is $g \in F$ such that $g(\alpha) = \beta$. If α is a dyadic rational then β is also a dyadic rational and the conclusion of the lemma holds. Otherwise $g(t) = 2^r t + 2^s w$ inside a small open neighborhood of α , for some $r, s, w \in \mathbb{Z}$. Let

$\alpha = \frac{2^t m}{n}, \beta = \frac{2^k u}{v}$, for some $t, k \in \mathbb{Z}$, $(m, n) = (u, v) = 1$, m, n, u, v odd. Then

$$\frac{2^k u}{v} = \beta = g(\alpha) = 2^r \frac{2^t m}{n} + 2^s w = \frac{2^{r+t} m + 2^s w n}{n}.$$

Now the numerator of $\frac{2^{r+t} m + 2^s w n}{n}$ and n may not be coprime any more, in which case we may cancel the common part and get a new odd part n' of the denominator of the right hand side. Moreover we have $v|n$. Applying the same argument for g^{-1} we have that $n|v$, i.e., $v = n$. Thus, if there is a g carrying α to β , then

$$u = 2^{r+t-k} m + 2^{s-k} w n$$

Now we can rename $R := r + t - k$ so that the equation becomes

$$u \equiv 2^R m \pmod{n}$$

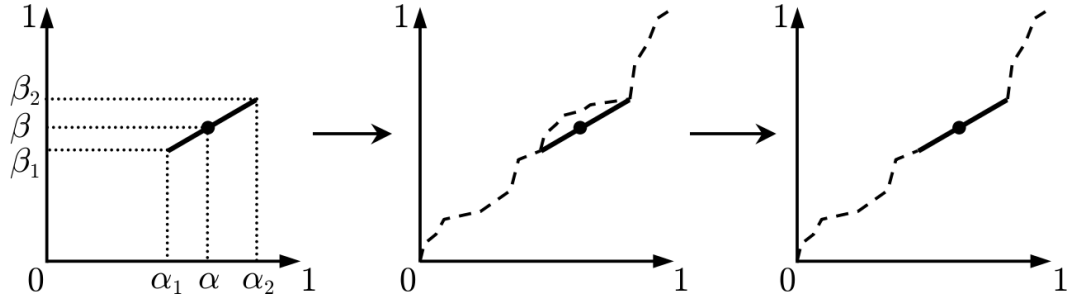


Figure 4.3: How to build a $g \in \text{PL}_2(I)$, with $g(\alpha) = \beta$.

Conversely, suppose u satisfies (4.1). Then we can find r, s, w such that, by going backwards in the "only if" argument, there is a small open interval $(\gamma, \delta) \subset [0, 1]$ containing α and a function $g(t) = 2^r t + 2^s w$, with $g(\alpha) = \beta$ and we can choose γ, δ so that they are dyadic rationals and $g(\gamma), g(\delta) \in I$. Now we just apply the extension Lemma 4.1.5 and extend g to the whole interval $[0, 1]$ (see figure 4.3).

□

Example Let $\alpha = \frac{1}{17}$, $\beta = \frac{13}{17}$ and $\gamma = \frac{3}{17}$. It is easy to see that we can find a $g \in \text{PL}_2(I)$ with $g(\alpha) = \beta$, but there is no $h \in \text{PL}_2(I)$ with $h(\alpha) = \gamma$. The same can

be determined applying Proposition 3.2.3, since the binary expansions of the previous numbers are $\alpha = 0.\overline{00001111}, \beta = 0.11\overline{00001111}, \gamma = 00101101\overline{001011}$. \square

Corollary 4.1.7. *Given $\alpha, \beta \in \mathbb{Q} \cap (0, 1)$ there is an algorithm to determine whether or not there is a $g \in \text{PL}_2(I)$ such that $g(\alpha) = \beta$.*

Proof. In order to apply the previous proposition we need to check whether the odd parts of the denominator of α and β are the same and whether they satisfy condition (4.1). Equation (4.1) is solvable if and only the equation $2^X u = 2^Y m + 2^Z wn$, for some $X, Y, Z \in \mathbb{N}$, $w \in \mathbb{Z}$, is solvable. This last equation in turn is solvable if and only if we can solve

$$2^{X-Y} u \equiv m \pmod{n}, \quad (4.2)$$

because 2 and n are coprime integers, and so 2 is invertible in $\mathbb{Z}/n\mathbb{Z}$. If ϕ denotes Euler's function then we have that $2^{\phi(n)} \equiv 1 \pmod{n}$. Thus, to see if (4.2) is solvable, we just need to plug in all the possible $X - Y \in \{0, 1, \dots, \phi(n)\}$. \square

The previous Corollary is another interpretation of Proposition 3.2.3: in fact it tells us how to determine if the tail of the binary expansions of two rational numbers are the same. We now state the same results for a finite number of points. Its proof uses the extension Lemma 4.1.5 on a number of disjoint intervals, one around each point.

Corollary 4.1.8. *Let $0 < \alpha_1 < \dots < \alpha_r < 1$ and $0 < \beta_1 < \dots < \beta_r < 1$ be two rational partitions of $[0, 1]$. There exists a $g \in \text{PL}_2(I)$ with $g(\alpha_i) = \beta_i$ if and only if there are $g_1, \dots, g_r \in \text{PL}_2(I)$ such that $g_i(\alpha_i) = \beta_i$. Moreover, if such element g exists it can be constructed.*

Proof of Theorem 4.1.4. Using the previous Lemma we can determine whether or not we can make $\partial D(y)$ and $\partial D(z)$ coincide. First we have to check if $\# \partial D(y) =$

$\# \partial D(z)$. Then we use the previous Corollary to find a $g \in \text{PL}_2(I)$, with $g(\partial D(y)) = \partial D(z)$, if it exists. Let $\widehat{y} := g^{-1}yg$. Now we just have to check if the sets where the graphs of the two functions \widehat{y} and z intersect the diagonal are the same. In fact, we know that the boundary points of these sets are the same, so it is enough to check whether $D(\widehat{y})$ contains the same intervals as $D(z)$. \square

4.1.2 The Linearity Boxes

The very first thing to check, if y and z are to be conjugate through a $g \in \text{PL}_2(J)$, is whether they can be made to coincide in neighborhoods of the endpoints of $J = [\eta, \zeta]$. This subsection and the following one will deal with functions in $\text{PL}_+(J)$: we will reuse them in the discussion on $\text{PL}_{S,G}(I)$. We start by making the following observation: the map $\text{PL}_+(J) \rightarrow \mathbb{R}_+$ which sends a function f to $f'(\eta^+)$ is a group homomorphism.

Lemma 4.1.9. *Given three functions $y, z, g \in \text{PL}_+(J)$ such that $g^{-1}yg = z$, there exist $\alpha, \beta \in (\eta, \zeta)$ such that $y(t) = z(t)$, for all $t \in [\eta, \alpha] \cup [\beta, \zeta]$ (refer to figure 4.4).*

Proof. We prove the Lemma for the first interval. Let $\varepsilon > 0$ be a number small enough that

$$\begin{aligned} g(t) - \eta &= a(t - \eta), & \text{for } t \in [\eta, \eta + \varepsilon], \\ y(t) - \eta &= b(t - \eta), & \text{for } t \in [\eta, g(\eta + \varepsilon)], \\ g^{-1}(t) - \eta &= a^{-1}(t - \eta), & \text{for } t \in [\eta, yg(\eta + \varepsilon)]. \end{aligned}$$

for some $a, b > 0$. Let $\alpha = \min\{\eta + \varepsilon, g(\eta + \varepsilon), yg(\eta + \varepsilon)\}$. Then, for $t \in [\eta, \alpha]$, we have

$$z(t) = g^{-1}yg(t) - \eta = a^{-1}ba(t - \eta) = b(t - \eta) = y(t).$$

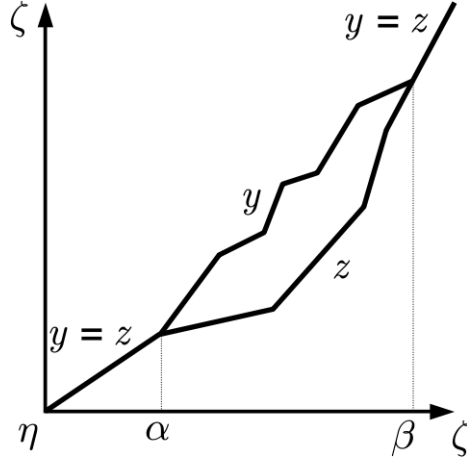


Figure 4.4: y and z coincide around the endpoints.

The second interval is found in the same way, after recentering the axis at the point (ζ, ζ) . \square

If two functions coincide at the beginning and at the end, then a candidate conjugator g will have to be linear in certain particular “boxes”, which depend only on y and z .

Lemma 4.1.10 (Initial Box). *Suppose $y, z, g \in \text{PL}_+(J)$ and $g^{-1}yg = z$. Let $\alpha > 0$ and $y'(\eta^+) = z'(\eta^+) = c > 1$ satisfy*

$$y(t) - \eta = z(t) - \eta = c(t - \eta) \text{ for } t \in [\eta, \eta + \alpha].$$

Then the graph of g is linear inside the square $[\eta, \eta + \alpha] \times [\eta, \eta + \alpha]$, i.e., the graph of g is linear in some neighborhood of the point (η, η) in $J \times J$ depending only on y and z (see figure 4.5).

Proof. We can rewrite the conclusion of this lemma, by saying that, if we define

$$\varepsilon = \sup\{r \mid g \text{ is linear on } [\eta, \eta + r]\},$$

then $\eta + \varepsilon \geq \min\{g^{-1}(\eta + \alpha), \eta + \alpha\}$. Assume the contrary, let $\varepsilon < \alpha$ and $\eta + \varepsilon < g^{-1}(\eta + \alpha)$ and write $g(t) - \eta = \gamma(t - \eta)$ for $t \in [\eta, \eta + \varepsilon]$, for some constant $\gamma > 0$. Let $0 \leq \sigma < 1$ be any number. Since $\sigma < 1$ and $\varepsilon < \alpha$, we have $\eta + \sigma\varepsilon < \eta + \alpha$ and so y is linear around $\eta + \sigma\varepsilon$:

$$g(y(\eta + \sigma\varepsilon)) = g(\eta + c\sigma\varepsilon).$$

On the other hand, since $\eta + \varepsilon < g^{-1}(\eta + \alpha)$, it follows that $g(\eta + \sigma\varepsilon) < g(\eta + \varepsilon) < \eta + \alpha$ and so z is linear around the point $g(\eta + \sigma\varepsilon) = \eta + \gamma\sigma\varepsilon$:

$$z(g(\eta + \sigma\varepsilon)) = z(\eta + \gamma\sigma\varepsilon) = \eta + c\gamma\sigma\varepsilon.$$

Since $gy = zg$, we can equate the previous two equations and write $g(\eta + c\sigma\varepsilon) = \eta + \gamma c\sigma\varepsilon$, for any number $0 \leq \sigma < 1$. If we choose $1/c < \sigma < 1$, we see that g must be linear on the interval $[0, c\sigma\varepsilon]$, where $c\sigma\varepsilon > \varepsilon$. This is a contradiction to the definition of ε . \square

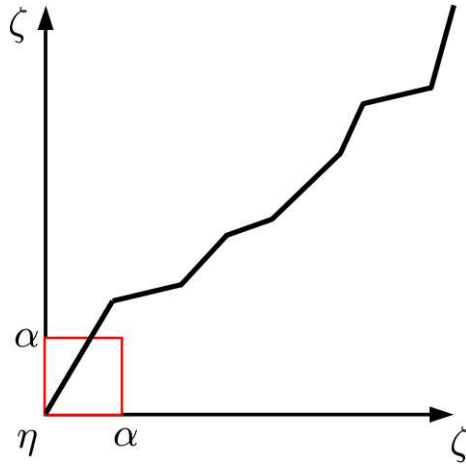


Figure 4.5: Initial linearity box.

Notice that the square neighborhood depends only on y and z . We observe that the Lemma also holds when $z'(\eta^+) = y'(\eta^+) = c < 1$ and the proof is given by applying the previous proof to the homeomorphisms y^{-1}, z^{-1} . Thus we can

remove any requirement on the initial slopes of y and z . Note that the Initial Box Lemma has an analogue for the points close to ζ :

Remark 4.1.11 (Final Box). Let $y, z, g \in \text{PL}_+(J)$. Suppose $(g^{-1}yg)(t) = y(t)$, for all $t \in J$. If there exist $\beta, c \in (0, 1)$ such that $y(t) = z(t) = c \cdot (t - \zeta) + \zeta$ on $[\beta, \zeta]$, then the graph of g is linear inside the square $[\beta, \zeta] \times [\beta, \zeta]$.

4.1.3 The Stair Algorithm for $\text{PL}_+^{\leq}(J)$

This subsection will deal with the main construction of this Chapter. We show how, under certain hypotheses, if there is a conjugator, then it is unique. On the other hand, we give a construction of such a conjugator, if it exists. Given two elements y, z the set of their conjugators is a coset of the centralizer of one of them, thus it makes sense to start by deriving properties of centralizers.

Lemma 4.1.12. *Let $z \in \text{PL}_+(J)$. Suppose there exist $\eta \leq \lambda \leq \mu \leq \zeta$ such that $z(t) \leq \lambda$, for every $t \in [\eta, \mu]$. Suppose further that $g \in \text{PL}_+(I)$ is such that*

(i) $g(t) = t$, for all $t \in [\eta, \lambda]$ and

(ii) $g^{-1}zg(t) = z(t)$, for all $t \in [\eta, \mu]$.

Then $g(t) = t$, for all $t \in [\eta, \mu]$.

Proof. Suppose, by contradiction, that there exist points $\lambda \leq \theta_1 < \theta_2 \leq \mu$ such that $g(t) = t$, for all $t \in [\eta, \theta_1]$ and $g(t) \neq t$ and g is linear, for $t \in (\theta_1, \theta_2]$. Recenter the axes in the point (θ_1, θ_1) through $T = t - \theta_1$ and $Z = z - \theta_1$. Then $g(t) = \alpha t$, for $t \in [0, \theta_2 - \theta_1]$, for some positive $\alpha \neq 1$ and $z(t) = \beta t - \gamma$, for $t \in [0, \varepsilon]$, for $\beta, \gamma \in \mathbb{R}$, $\varepsilon > 0$ suitable numbers. Observe that now $-\theta_1 \leq z(t) \leq z(\theta_2 - \theta_1) \leq \lambda - \theta_1 \leq 0$ and that

due to the recentering $g(t) = t$ on $[-\theta_1, 0]$. For any $0 < t < \min\{\theta_2 - \theta_1, \varepsilon, \varepsilon/\alpha\}$ the following equalities hold:

$$\beta t - \gamma = z(t) = gz(t) = zg(t) = z(\alpha t) = \alpha\beta t - \gamma,$$

and so this implies $\beta t = \alpha\beta t$, hence $\alpha = 1$. Contradiction. \square

Corollary 4.1.13. *Let $z \in \text{PL}_+^<(J)$ and $g \in \text{PL}_+(J)$ be such that*

$$(i) \ g'(\eta^+) = 1,$$

$$(ii) \ g^{-1}zg(t) = z(t), \text{ for all } t \in J.$$

Then $g(t) = t$, for all $t \in J$.

Proof. Since $g'(\eta^+) = 1$, we have $g(t) = t$ in an open neighborhood of η . Suppose, to set a contradiction, that $g(t_0) \neq t_0$, for some $t_0 \in (\eta, \zeta)$. Let λ be the first point after which $g(t) \neq t$. It is obvious that $\eta < \lambda < \zeta$. Thus $z(\lambda) < \lambda$ and we let $\mu = z^{-1}(\lambda) > \lambda$. So we have that $z(t) \leq \lambda$ on $[0, \mu]$, $g(t) = t$ on $[\eta, \lambda]$ and $g^{-1}zg = z$ on I . By the previous Lemma, $g(t) = t$ on $[\eta, \mu]$, with $\mu > \lambda$. Contradiction. \square

Lemma 4.1.14. *Let $z \in \text{PL}_0^<(J)$. Let $C_{\text{PL}_+(J)}(z)$ be the centralizer of z in $\text{PL}_+(J)$.*

Define the map

$$\begin{aligned} \varphi_z : C_{\text{PL}_+(J)}(z) &\longrightarrow \mathbb{R}_+ \\ g &\longmapsto g'(\eta^+). \end{aligned}$$

Then φ_z is an injective group homomorphism.

Proof Let $y \in \text{PL}_0^<(J)$ and suppose that there exists two elements $g_1, g_2 \in C_{\text{PL}_+(J)}(y)$ such that $\varphi_y(g_1) = \varphi_y(g_2)$, then $g_1^{-1}g_2$ has a slope 1 near η and by the previous Lemma is equal to the identity. Therefore $g_1 = g_2$, which proves the injectivity. Clearly this is a group homomorphism. \square

The Lemma implies the following:

Lemma 4.1.15. *Let $y, z \in \text{PL}_0^<(J)$, let $C_{\text{PL}_+(J)}(y, z) = \{g \in \text{PL}_+(J) \mid y^g = z\}$ be the set of all conjugators and let λ be in the interior of J . We define the following two maps*

$$\begin{aligned} \varphi_{y,z} : C_{\text{PL}_+(J)}(y, z) &\longrightarrow \mathbb{R}_+ \\ g &\longmapsto g'(\eta^+) \\ \psi_{y,z,\lambda} : C_{\text{PL}_+(J)}(y, z) &\longrightarrow J \\ g &\longmapsto g(\lambda). \end{aligned}$$

Then

(i) $\varphi_{y,z}$ is an injective map.

(ii) There is a map $\rho_\lambda : J \rightarrow \mathbb{R}_+$ such that the following diagram commutes:

$$\begin{array}{ccc} C_{\text{PL}_+(J)}(y, z) & \xrightarrow{\varphi_{y,z}} & \mathbb{R}_+ \\ & \searrow \psi_{y,z,\lambda} & \uparrow \rho_\lambda \\ & & J \end{array}$$

(iii) $\psi_{y,z,\lambda}$ is injective.

Proof. (i) is an immediate corollary of Lemma 4.1.14. (ii) Without loss of generality we can assume that the initial slopes of y, z are the same (otherwise the set $C_{\text{PL}_+(J)}(y, z)$ is obviously empty and any map will do). We define the map $\rho_\lambda : J \rightarrow \mathbb{R}_+$ as

$$\rho_\lambda(\mu) = \lim_{n \rightarrow \infty} \frac{y^n(\mu) - \eta}{z^n(\lambda) - \eta}$$

We observe that the limit exists, i.e. the sequence stabilizes under these assumptions.

To prove that the diagram commutes we define $\mu = g(\lambda)$ and observe that $y^n(\mu) \xrightarrow{n \rightarrow \infty} \eta$ and $z^n(\lambda) \xrightarrow{n \rightarrow \infty} \eta$. By hypothesis $y(\mu) = g(z(\lambda))$ so that $g(z^n(\lambda)) = y^n(\mu)$, for every $n \in \mathbb{Z}$. Since g fixes η we have

$$g(t) = g'(\eta^+)(t - \eta) + \eta \text{ on a small interval } [\eta, \eta + \varepsilon],$$

where ε depends on g . Let $N = N(g) \in \mathbb{N}$ be large enough, so that the numbers $y^N(\lambda), z^N(\lambda) \in (\eta, \eta + \varepsilon)$. This implies that, for any $n \geq N$

$$y^n(\mu) = g(z^n(\lambda)) = g'(\eta^+)(z^n(\lambda) - \eta) + \eta$$

and so then

$$\varphi_{y,z}(g) = g'(\eta^+) = \frac{y^n(\mu) - \eta}{z^n(\lambda) - \eta} = \rho_\lambda(\psi_{y,z,\lambda}(g)).$$

(iii) Since $\varphi_{y,z} = \rho_\lambda \psi_{y,z,\lambda}$ is injective by part (i), then $\psi_{y,z,\lambda}$ is also injective. \square

Our strategy will be to construct a “section” of the map $\varphi_{y,z}$, if it exists. Then as a consequence we will build a “section” of the map $\psi_{y,z,\lambda}$ too. The main tool of this subsection is the **Stair Algorithm**. This procedure builds a conjugator (if it exists) with a given fixed initial slope. The idea of the algorithm is the following. In order for y and z to be conjugate, they must have the same initial slope; by the initial linearity box Lemma this determines uniquely the first piece of a possible conjugator. Then we “walk up the first step of the stair”, with the Identification Trick, that is basically identifying y and z inside a rectangle next to the linearity box, by taking a suitable product of y and z as a conjugator. Then we repeat and walk up more rectangles, until we “reach the door” (represented by the final linearity box) and this happens when a rectangle that we are building crosses the final linearity box.

Lemma 4.1.16 (Identification Trick). *Let $y, z \in \text{PL}_+^<(J)$ and let $\alpha \in (\eta, \zeta)$ be such that $y(t) = z(t)$ for $t \in [\eta, \alpha]$. Then there exists a $g \in \text{PL}_+(I)$ such that $z(t) = y^g(t)$ for*

$t \in [\eta, z^{-1}(\alpha)]$ and $g(t) = t$ in $[\eta, \alpha]$. The element g is uniquely defined up to the point $z^{-1}(\alpha)$. If $y, z \in \text{PL}_2^{\leq}(J)$ then g can be chosen in $\text{PL}_2(J)$ (see figure 4.6).

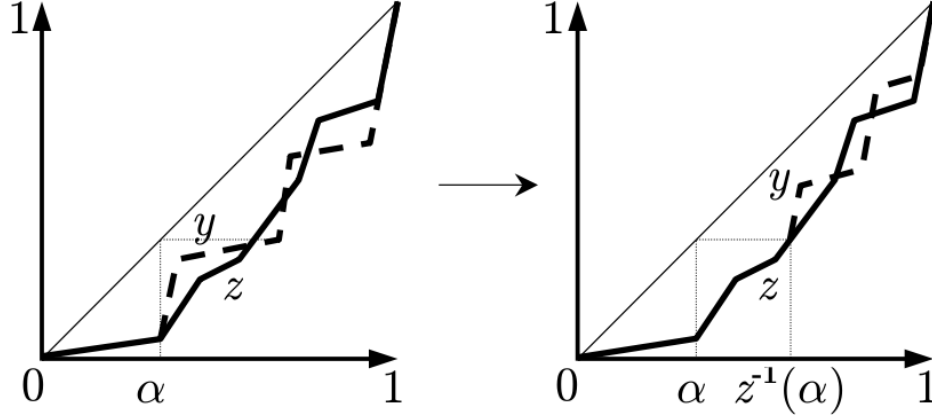


Figure 4.6: The identification trick

Proof. If such g exists then we have that, for $t \in [\eta, z^{-1}(\alpha)]$

$$y(g(t)) = g(z(t)) = z(t)$$

since $z(t) \leq \alpha$ in $[\eta, z^{-1}(\alpha)]$. Thus, for $t \in [\alpha, z^{-1}(\alpha)]$, we have that $g(t) = y^{-1}z(t)$.

Now, that we have derived this necessary condition, we are ready to prove that such a g exists. Now define

$$g(t) := \begin{cases} t & t \in [\eta, \alpha] \\ y^{-1}z(t) & t \in [\alpha, z^{-1}(\alpha)]. \end{cases}$$

and extend it to J as a line from the point $(z^{-1}(\alpha), y^{-1}(\alpha))$ to (ζ, ζ) . If $y, z \in \text{PL}_2(J)$ then we extend g to J , through the extension Lemma. A direct computation verifies that $y^g(t) = z(t)$ for $t \in z^{-1}(\alpha)$. \square

Proposition 4.1.17 (Stair Algorithm for $\text{PL}_+^{\leq}(J)$). *Let $y, z \in \text{PL}_+^{\leq}(J)$ and let q be a fixed positive real number. We can decide whether or not there is a $g \in \text{PL}_+(I)$ with initial slope $g'(\eta^+) = q$ such that $y^g = z$. If g exists, it is unique and can be constructed.*

Proof. Assume $y \neq z$ and, up to taking inverses, suppose $0 < g'(\eta^+) = q < 1$. Let $[\eta, \alpha]^2$ the initial linearity box and $[\beta, \zeta]^2$ the final one. Then, for y and z to be conjugate we must have that g has is linear in $[\eta, \alpha]^2$ and in $[\beta, \zeta]^2$. Since $q < 1$ we must have g linear on the interval $[\eta, \alpha]$ and so we define:

$$g_0(t) := q(t - \eta) + \eta \quad t \in [\eta, \alpha].$$

and extend it to the whole J . Now take the function $y_1 = g_0^{-1}yg_0$, which is still below the diagonal. Our goal now is to see if y_1 and z are conjugate. What is different now is that the new conjugator we will try to build is the identity on $[\eta, \alpha]$, where we already know that the functions y_1 and z coincide. We use the Identification Trick under the diagonal and build

$$g_1(t) := \begin{cases} t & t \in [\eta, \alpha] \\ y_1^{-1}z(t) & t \in [\alpha, z^{-1}(\alpha)] \end{cases}$$

then extending it to J . Again, we want to see we can find a conjugator of y_2 and z such that it is the identity on $[\eta, z^{-1}(\alpha)]$. Thus if we iterate this process and we build a sequence $g_2, y_3, g_3, \dots, y_r, g_r, \dots$. By construction, we always have that g_r is the identity on $[\eta, z^{-r}(\alpha)]$ and that $y_r(t) = z(t)$ for all $t \in [\eta, z^{-r}(\alpha)]$. We apply Lemma 4.1.19 and choose the smallest integer r so that

$$\min\{z^{-r}(\alpha), y^{-r}(\eta + q(\alpha - \eta))\} > \beta$$

and notice that this r depends *only* on y, z and q . Observe now that the Identification Trick tells us that, if the function g of the statement exists, it must coincide with the function $h(t) := g_0 \dots g_r(t)$, for $t \in [\eta, z^{-r}(\alpha)]$. If we prove that the part of the graph of h on the interval $[z^{-r}(\alpha), 1]$ is inside the final box, then we can build g by extending it linearly up to the point (ζ, ζ) . Recall that, by construction $g_{i-1}y_i^{-1} = y_{i-1}^{-1}g_{i-1}$ and $g_i(z^{-i}(\alpha)) = y_i^{-1}(z^{-i+1}(\alpha))$, for all $i = 1, \dots, r$. Then

$$\begin{aligned}
h(z^{-r}(\alpha)) &= g_0 \dots g_{r-2} y_{r-1}^{-1} g_{r-1} (z^{-r+1}(\alpha)) = \\
&= g_0 \dots g_{r-2} y_{r-1}^{-2} (z^{-r+2}(\alpha)) = \dots = \\
&= y^{-r} g_0(\alpha) = y^{-r}(\eta + q(\alpha - \eta)) > \beta.
\end{aligned}$$

Since $z^{-r}(\alpha) > \beta$ by our choice of r then $(z^{-r}(\alpha), h(z^{-r}(\alpha))) \in [\beta, \zeta]^2$ and therefore we can define g by extending it linearly in the last segment, i.e. joining $(z^{-r}(\alpha), h(z^{-r}(\alpha)))$ with $(1, 1)$.

If the function h is not linear on $[\beta, z^{-r}(\alpha)]$, then there is no conjugator for y and z . Otherwise, we have to check whether $g^{-1}yg = z$ and we are done. To prove the uniqueness of g , we just apply Lemma 4.1.15. \square

Lemma 4.1.18. *Let $y, z \in \text{PL}_+^<(J)$, $g \in \text{PL}_+(J)$ and $n \in \mathbb{N}$. Then $g^{-1}yg = z$ if and only if $g^{-1}y^n g = z^n$.*

Proof. The “only if” part is obvious. The “if” part follows from the injectivity of φ_x of Lemma 4.1.14 since $g^{-1}yg$ and z both centralize the element $g^{-1}y^n g = z^n$. \square

Lemma 4.1.19. *Let $J = [\eta, \zeta]$ be a compact interval, let $y, z \in \text{PL}_+^<(J)$ and $g \in \text{PL}_+(J)$ be such that $g^{-1}yg = z$. Suppose moreover that $[\eta, \alpha] \times [\eta, \alpha]$ is the initial linearity box and $[\beta, \zeta] \times [\beta, \zeta]$ is the final one for y and z . For every positive real number q there is a $k \in \mathbb{N}$ such that $y^k(\beta) < \eta + q(\alpha - \eta)$, $z^k(\beta) < \alpha$. Moreover y^k and z^k are still conjugate through g , so g must still be linear in the same linearity boxes of y and z .*

Proof. Since $y(\beta) < \beta$ and $y \in \text{PL}_+^<(J)$ then $y^n(\beta) \xrightarrow{n \rightarrow \infty} \eta$. Similarly this is true for $\{z^n(\beta)\}$ and so we can pick any number $r \in \mathbb{N}$ big enough to satisfy the statement.

Moreover, we have $g^{-1}y^k g = (g^{-1}yg)^k = z^k$. Finally we observe that the linearity box of y^r and z^r is smaller than that of y and z , but that we already know that g has to be linear on $[\eta, \alpha]$ and on $[\beta, \zeta]$. \square

The stair algorithm can also be proved in a slightly different way. We can apply Lemma 4.1.19 at the beginning and work with y^r and z^r instead of y and z . This gives a proof which concludes in two steps, although it yields the same complexity for a machine which has to compute immediately the powers y^r and z^r .

“Short” Proof of Proposition 4.1.17. Assume the same setting of the Proposition 4.1.17. We choose r to be the smallest number satisfying Lemma 4.1.19, so that

$$\min\{z^{-r}(\alpha), y^{-r}(\eta + q(\alpha - \eta))\} > \beta$$

If we call $\widehat{z} = z^r$ and $\widehat{y} = y^r$ then we have:

$$\min\{\widehat{z}^{-1}(\alpha), \widehat{y}^{-1}(\eta + q(\alpha - \eta))\} > \beta.$$

With this assumption, the algorithm we are going to define will need only two steps to end. We define g_0 as before. Then we define $\widehat{y}_1 = g_0^{-1}\widehat{y}g_0$ and we define a map g_1 as in the previous proof out of \widehat{y}_1 . Now we observe that g_0g_1 is a conjugator up to the point $\widehat{z}^{-1}(\alpha)$ and that it enters the final linearity box, as in the previous proof. Now we extend it by linearity and we check whether this is a conjugator. If it is, it is the unique one. \square

Remark 4.1.20. By the uniqueness of the conjugator (Lemma 4.1.15) we remark that both the proofs of the stair algorithm do not depend on the choice of g_0 . The only requirements on g_0 are that it must be linear in the initial box and $g'_0(\eta^+) = q$.

Corollary 4.1.21 (Explicit Conjugator). *Let $y, z \in \text{PL}_+^<(J)$, let $[\eta, \alpha]$ be the initial linearity box and let q be a positive real number. There is an $r \in \mathbb{N}$ such that the*

unique candidate conjugator with initial slope $q < 1$ is given by

$$g(t) = y^{-r} g_0 z^r(t) \quad \forall t \in [\eta, z^{-r}(\alpha)]$$

and linear otherwise, where g_0 is any map in $\text{PL}_+(J)$ which is linear in the initial box and such that $g'_0(\eta^+) = q$.

Proof. We run the short stair algorithm and let $g = g_0 g_1$ be defined as above. By the short proof of the stair algorithm and the previous Remark, we have $g = g_0 g_1 = y^{-1} g_0 g_1 z$ on $[\eta, z^{-r}(\alpha)]$ for some r . Therefore

$$g(t) = y^{-r} g_0 g_1 z^{-r}(t) = y^{-r} g_0 z^r(t) \quad \forall t \in [\eta, z^{-r}(\alpha)]$$

and it is linear on $[z^{-r}(\alpha), \zeta]$. \square

Corollary 4.1.22. *Let $y, z \in \text{PL}_+^<(J)$, and let λ be in the interior of J . The map*

$$\begin{aligned} \psi_{y,z,\lambda} : C_{\text{PL}_+(J)}(y, z) &\longrightarrow J \\ g &\longmapsto g(\lambda). \end{aligned}$$

admits a section, i.e. if $\psi_{y,z,\lambda}(g) = \mu \in J$, then g is unique and can be constructed.

Remark 4.1.23. Suppose $y, z \in \text{PL}_+^<(J) \cup \text{PL}_+^>(J)$, then in order to be conjugate, they will have to be both in $\text{PL}_+^<(J)$ or both in $\text{PL}_+^>(J)$, because by Lemma 4.1.9 they will have to coincide in a small interval $[\eta, \alpha]$. Moreover, $g^{-1}yg = z$ if and only if $g^{-1}y^{-1}g = z^{-1}$, and so, up to working with y^{-1}, z^{-1} , we may reduce to studying the case where they are both in $\text{PL}_+^<(J)$.

Remark 4.1.24 (Backwards Stair Algorithm). The stair algorithm for $\text{PL}_+^<(J)$ can be reversed. This is to say that, given q a positive real number, we can determine whether or not there is a conjugator g with final slope $g'(\zeta^-) = q$. The proof is the same: we simply start building g from the final box.

Remark 4.1.25. All the results of subsections 4.1.2 and 4.1.3 can be stated and proved by substituting $\text{PL}_2(J)$ and $\text{PL}_2^{\leq}(J)$ for every appearance of $\text{PL}_+(J)$ and $\text{PL}_+^{\leq}(J)$. Only a few more remarks must be made in order to prove it. In the Identification Trick we need to observe that α and $z^{-1}(\alpha)$ are dyadic and to take all the extensions in $\text{PL}_2(J)$ through the extension Lemma.

The stair algorithm gives a practical way to find conjugators if they exist and we have chosen a possible initial slope. By modifying the algorithm we can see that, if two elements are in $\text{PL}_2^{\leq}(J)$ and they are conjugate through an element with initial slope a power of 2 then the conjugator is an element of $\text{PL}_2(J)$.

Corollary 4.1.26. *Let $y, z \in \text{PL}_2^{\leq}(J)$, $g \in \text{PL}_+(J)$ such that $y^g = z$ and $g'(\eta^+)$ is a power of 2. Then $g \in \text{PL}_2(J)$.*

4.1.4 The Stair Algorithm and the Mather Invariant

In Subsection 3.3.2 we have defined the Mather invariant for elements of $\text{PL}_2^{\geq}(I)$. For an element $f \in \text{PL}_2^{\geq}(I)$, the invariant f^{∞} is defined by taking large powers of f and then taking a quotient so that f^{∞} is a map from the quotient space of a neighborhood of 0 to the quotient space of a neighborhood of 1 (they both become circles). The Mather invariant can be represented as an annular strand diagram or an unlabeled cylindrical strand diagram (see figure 4.7).

In Corollary 4.1.21 the Stair Algorithm yields that two elements $y, z \in \text{PL}_2^{\geq}(I)$ are conjugate if and only if the map $y^{-r}g_0z^r$ is a conjugator, for an integer r large enough and for any element $g_0 \in \text{PL}_2^{\geq}(I)$ with a given initial slope. We observe that if there is a conjugator g it is thus equal to $y^{-N}g_0z^N$ for any integer $N \geq r$. The

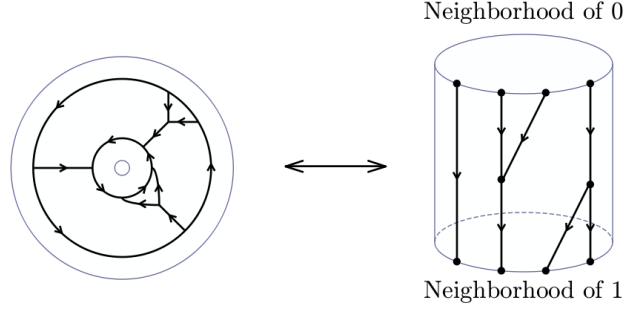


Figure 4.7: Mather invariant as an unlabeled cylindrical strand diagram

parallel between the two descriptions is now more apparent. If we take N very large, the two maps y^N and z^N can be seen as the Mather invariants for y and z . We can rewrite the equation as

$$y^N g = g_0 z^N.$$

If we pass to quotients, what we see on the left hand side is the composition of the Mather invariant y^∞ by the map g which acts as a rotation on the domain circle of y^∞ . On the right hand side, we see the composition of a rotation of the range circle of z^∞ by the Mather invariant z^∞ . This can also be visualized in figure 4.8.

We recall that, by Theorem 3.3.6, y and z are conjugate if and only if their Mather invariants differ by a rotation in the domain and the range, and this is precisely the same result that we obtain from Corollary 4.1.21, and the two points of view agree.

Remark 4.1.27. The previous discussion does not depend from the point of view of strand diagrams (they only provide a different way to visualize it). The parallel between the formula for the explicit conjugator of Corollary 4.1.21 and the definition of Mather Invariants for functions of $\text{PL}_+^>(I)$ is shown by the cube diagram contained in the proof of the Brin-Squier Theorem 3.3.3. Hence the paral-

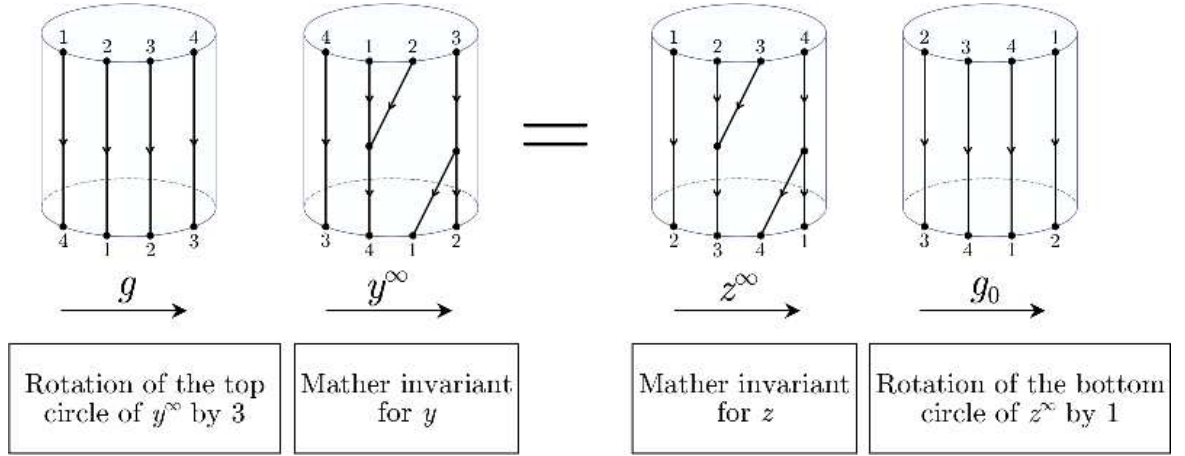


Figure 4.8: Cylindrical strand diagrams “differ” by a rotation on the top or on the bottom

lel between the two points of view can be generalized to $\text{PL}_+(I)$ and later on to the groups $\text{PL}_{S,G}(I)$ (in Section 4.4 we will generalize the Stair Algorithm to the groups $\text{PL}_{S,G}(I)$).

4.1.5 The Stair Algorithm for $\text{PL}_2^0(J)$

Subsection 4.1.1 proves that we can reduce our study to y and z such that $\partial D(y) = \partial D(z)$. It is now important to notice that an intersection point α of the graph of z with the diagonal may not be a dyadic rational. If this is the case then α cannot be a breakpoint for y, z, g . This means that, for these α 's, we have that $y'(\alpha), z'(\alpha)$ and $g'(\alpha)$ are defined, i.e., the left and right derivatives coincide. Recall that a function z belongs to the set $\text{PL}_2^0(J)$ if its graph does not have dyadic intersection points with the diagonal.

Proposition 4.1.28 (Stair Algorithm for $\text{PL}_2^0(J)$). *Let $y, z \in \text{PL}_2^0(J)$ and suppose that $\partial D(y) = \partial D(z)$. Let q be a fixed power of 2. We can decide whether or not*

there is a $g \in \text{PL}_2(J)$ with initial slope $g'(\eta^+) = q$ such that y is conjugate to z through g . If g exists it is unique.

Proof. This proof will be essentially the same as the previous stair algorithm with a few more remarks. We assume therefore that such a conjugator exists and build it. Let $\partial D(y) = \partial D(z) = \{\eta = \alpha_0 < \alpha_1 < \dots < \alpha_s < \alpha_{s+1} = \zeta\}$. We restrict our attention to $\text{PL}_2([\alpha_i, \alpha_{i+1}])$, for each $i = 0, \dots, s$. If y and z are conjugate on $[\alpha_i, \alpha_{i+1}]$ then we can speak of linearity boxes: let $\Gamma_i := [\alpha_i, \gamma_i] \times [\alpha_i, \gamma_i]$ be the initial linearity box and $\Delta_i := [\delta_i, \alpha_{i+1}] \times [\delta_i, \alpha_{i+1}]$ the final one for $\text{PL}_2([\alpha_i, \alpha_{i+1}])$. Now what is left to do is to repeat the procedure of the stair algorithm for elements in $\text{PL}_2^<(U)$, for some interval U . We build a conjugator g on $[\alpha_0, \alpha_1]$ by means of the stair algorithm. We observe that α_1 is not a breakpoint, hence $g'(\alpha_1^+) = g'(\alpha_1^-)$. Thus we are given an initial slope for g in $[\alpha_1, \alpha_2]$, then we can repeat the same procedure and repeat the stair algorithm on $[\alpha_1, \alpha_2]$. We keep repeating the same procedure until we reach $\alpha_{s+1} = \zeta$. Then we check whether the g we have found conjugates y to z . Finally, we observe that in each square $[\alpha_i, \alpha_{i+1}] \times [\alpha_i, \alpha_{i+1}]$ the determined function is unique, since we can apply Lemma 4.1.15 on it. \square

An immediate consequence of the previous result is the following Lemma:

Lemma 4.1.29. *Suppose $z \in \text{PL}_2^0(J)$ and $g \in \text{PL}_2(J)$ are such that*

- (i) $g'(\eta^+) = 1$,
- (ii) $(g^{-1}zg)(t) = z(t)$, for all $t \in J$.

Then $g(t) = t$, for all $t \in J$.

Remark 4.1.30 (Backwards and Midpoint Stair Algorithm). It is possible to run a backwards version of the stair algorithm also for $\text{PL}_2^0(J)$. Moreover, in this case

it also possible to run a midpoint version of it: if we are given a point λ in the interior of J fixed by y and z and q a fixed power of 2, then, by running the stair algorithm at the left and the right of λ we determine whether there is or not a conjugator g such that $g'(\lambda) = q$.

From the previous Lemma and Remark it is immediate to derive:

Corollary 4.1.31. *Let $y, z \in \text{PL}_2^0(J)$ such that $D(y) = D(z)$ and let $C_{\text{PL}_2(J)}(y, z) = \{g \in \text{PL}_2(J) \mid y^g = z\}$ be the set of all conjugators. For any $\tau \in D(y)$ define the map*

$$\begin{aligned} \varphi_{y,z,\tau} : C_{\text{PL}_2(J)}(y, z) &\longrightarrow \mathbb{R}_+ \\ g &\longmapsto g'(\tau), \end{aligned}$$

where if τ is an endpoint of J we take only a one-sided derivative. Then

(i) $\varphi_{y,z,\tau}$ is an injective map.

(ii) If $\varphi_{y,z,\tau}$ admits a section, i.e. if there is a map $\mathbb{R}_+ \rightarrow C_{\text{PL}_2(J)}(y, z)$, $\mu \rightarrow g_\mu$ such that $\varphi_{y,z,\tau}(g_\mu) = \mu$ then g_μ is unique and can be constructed.

Proposition 4.1.32. *Let $y, z \in \text{PL}_2^0(J)$ such that $D(y) = D(z)$ and let λ be in the interior of J such that $y(\lambda) \neq \lambda$. Define*

$$\begin{aligned} \psi_{y,z,\lambda} : C_{\text{PL}_+(J)}(y, z) &\longrightarrow J \\ g &\longmapsto g(\lambda). \end{aligned}$$

Suppose $y^n(\lambda) \xrightarrow{n \rightarrow \infty} \tau$. Then

(i) There is a map $\rho_\lambda : J \rightarrow \mathbb{R}_+$ such that the following diagram commutes:

$$\begin{array}{ccc} C_{\text{PL}_+(J)}(y, z) & \xrightarrow{\varphi_{y,z,\tau}} & \mathbb{R}_+ \\ & \searrow \psi_{y,z,\lambda} & \uparrow \rho_\lambda \\ & & J \end{array}$$

(ii) $\psi_{y,z,\lambda}$ is injective.

(iii) If $\psi_{y,z,\lambda}$ admits a section, i.e. if there is a map $J \rightarrow C_{\text{PL}_2(I)}(y, z)$, $\mu \rightarrow g_\mu$ such that $\psi_{y,z,\lambda}(g_\mu) = \mu$ then g_μ is unique and can be constructed.

Proof. Let $D(y) = D(z) = \{\eta = \mu_0 < \mu_1 < \dots < \mu_k < \mu_{k+1} = \zeta\}$ and suppose $\mu_i < \lambda < \mu_{i+1}$ for some i . We define the partial map $\rho_\lambda : J \rightarrow \mathbb{R}_+$ as

$$\rho_\lambda(\mu) = \begin{cases} \lim_{n \rightarrow \infty} \frac{y^n(\mu) - \tau}{z^n(\lambda) - \tau} & \mu \in [\mu_i, \mu_{i+1}] \\ 1 & \text{otherwise} \end{cases}$$

Since $D(y) = D(z)$, $z^n(\lambda) \xrightarrow{n \rightarrow \infty} \tau$ and τ is fixed by g . Thus if $\mu = g(\lambda)$, then $y^n(\mu) = g(z^n(\lambda)) \xrightarrow{n \rightarrow \infty} \tau$. With this definition, the proof follows closely that of Lemma 4.1.15(ii), Proposition 4.1.22 and by applying Corollary 4.1.31 and the previous Remark. \square

We conclude this subsection with a technical lemma which we will need later on:

Lemma 4.1.33. *Let $\tau, \mu \in J$, $h \in \text{PL}_+(J)$. Then:*

(i) *The limit $\varphi_\pm = \lim_{n \rightarrow \infty} h^{\pm n}(\tau)$ exists and $h(\varphi_\pm) = \varphi_\pm$,*

(ii) *We can determine whether there is or not an $n \in \mathbb{Z}$, such that $h^n(\tau) = \mu$.*

Proof. If $h(\tau) = \tau$ then it is clear. Otherwise, without loss of generality, we can assume $h(\tau) > \tau$. The two sequences $\{h^{\pm n}(\tau)\}_{n \in \mathbb{N}}$ are strictly monotone, and they have a limit $\lim_{n \rightarrow \infty} h^{\pm n}(\tau) = \varphi_\pm \in [0, 1]$. Thus, by continuity of h

$$\varphi_\pm = \lim_{n \rightarrow \infty} h^{n+1}(\tau) = \lim_{n \rightarrow \infty} h(h^n(\tau)) = h(\varphi_\pm).$$

Thus we have that $\{h^n(\tau)\}_{n \in \mathbb{Z}} \subseteq (\varphi_-, \varphi_+)$ and we have that φ_+ is the closest intersection of h with the diagonal on the right of τ (similarly for φ_-), so we can

compute φ_+, φ_- directly, without using the limit. As a first check, we must see if $\mu \in (\varphi_-, \varphi_+)$. Then since the two sequences $\{h^{\pm n}(\tau)\}_{n \in \mathbb{N}}$ are monotone, then after a finite number of steps we find $n_1, n_2 \in \mathbb{Z}$ such that $h^{-n_1}(\tau) < \mu < h^{n_2}(\tau)$ and so this means that either there is an integer $-n_1 \leq n \leq n_2$ with $h^n(\tau) = \mu$ or not, but this is a finite check. \square

4.1.6 The conjugacy problem for $\text{PL}_2(I)$

We are now ready to give an alternative proof of the solvability of the ordinary conjugacy problem (compare it with Theorem 2.1.9).

Lemma 4.1.34. *For any $y, z \in \text{PL}_2^0(I)$ we can decide whether there is (or not) a $g \in \text{PL}_2(I)$ with $y^g = z$.*

Proof. Let $y, z \in \text{PL}_2(I)$, $y \neq z$. We use Theorem 4.1.4 to make $\partial D(y) = \partial D(z)$, if possible. In order to be conjugate, we must have $y'(0^+) = z'(0^+)$ and $y'(1^-) = z'(1^-)$. Up to taking inverses of y and z , we can assume that $2^u = y'(0^+) = z'(0^+) < 1$. Now observe that $g^{-1}yg = z$ is satisfied if and only if $(y^v g)^{-1}y(y^v g) = z$ is satisfied for every $v \in \mathbb{Z}$. If $2^{\rho(g)}$ is the initial slope of g , then $2^{vu+\rho(g)}$ is the initial slope of $y^v g$. Thus, up to taking powers of y , we can assume that the initial slope of g is between 2^u and 2^{-1} . Now we choose all $q \in U := \{2^u, 2^{u+1}, \dots, 2^{-1}\}$ as possible initial slopes for g , therefore we apply the stair algorithm for $\text{PL}_2^0(I)$ for all the elements of U and check if we find a solution or not. There is only a finite number of “possible” initial slopes, so the algorithm will terminate. Moreover, by Lemma 2.22 we can derive the uniqueness of each solution, for a given initial slope. \square

The previous Lemma provides a way to find all possible conjugators, however it is not an efficient way to do it because we are taking all possible slopes into consideration.

Theorem 4.1.35. *The group $\text{PL}_2(I)$ has solvable conjugacy problem.*

Proof. We use Theorem 4.1.4 again and suppose that $\partial_2 D(y) = \partial_2 D(z) = \{0 = \alpha_0 < \alpha_1 < \dots < \alpha_r < \alpha_{r+1} = 1\}$. Now we restrict to an interval $[\alpha_i, \alpha_{i+1}]$ and consider $y, z \in \text{PL}_2^0([\alpha_i, \alpha_{i+1}])$. If $D(y)$ contains the a subinterval of $[\alpha_i, \alpha_{i+1}]$, then we must have $y = z = id$ on the whole interval $[\alpha_i, \alpha_{i+1}]$ and so any function $g \in \text{PL}_2([\alpha_i, \alpha_{i+1}])$ will be a conjugator. Otherwise, $D(y)$ does not contain any subinterval of $[\alpha_i, \alpha_{i+1}]$ and so we can apply the previous Lemma on it. If we find a solution on each such interval, then the conjugacy problem is solvable. Otherwise, it is not. \square

The argument given to solve the conjugacy problem in F also works, in much the same way, to solve the power conjugacy problem. We say that a group G has *solvable power conjugacy problem* if there is an algorithm such that, given any two elements $y, z \in G$, we can determine whether there is, or not, a $g \in G$ and two non-zero integers m, n such that $g^{-1}y^mg = z^n$, that is, there are some powers of y and z that are conjugate.

Theorem 4.1.36. *The group $\text{PL}_2(I)$ has solvable power conjugacy problem.*

Proof. Again, we can use Theorem 4.1.4, suppose that $\partial_2 D(y) = \partial_2 D(z)$ and restrict to a smaller interval $J = [\eta, \zeta]$ with dyadic endpoints and such that $y, z \in \text{PL}_2^0(J)$. If $g \in \text{PL}_2(J)$ and m, n exist then we must have that the initial slope of y^m and z^n must coincide. A simple argument on the exponent of these slopes, implies that this can happen if and only if y^m and z^n are both powers of a common minimal

power $(y^\alpha)'(\eta) = (z^\beta)'(\eta)$. Hence the problem can be reduced to finding whether there is a $g \in \text{PL}_2(J)$ and an integer k such that $g^{-1}y^{k\alpha}g = z^{k\beta}$. By Lemma 4.1.18 (that can be naturally generalized to $\text{PL}_2^0(J)$), we have that this is equivalent to finding a $g \in \text{PL}_2(J)$ such that $g^{-1}y^\alpha g = z^\beta$. Hence solving the power conjugacy problem is equivalent to solving the conjugacy problem for y^α and z^β . \square

4.2 Roots and Centralizers in $\text{PL}_2(I)$

In this section we show how the techniques developed so far allow us to obtain two previously known results. The first of these results was first proved by Brin and Squier in [18] in 1985 and later proved again by Guba and Sapir in [38] in 1997. Most of the results of this section are proved in [38] using different methods.

Proposition 4.2.1 (Computing Roots). *Let $id \neq x \in \text{PL}_2(I)$, then the function x has only a finite number of roots and every root is constructible, i.e., there is an algorithm to compute it.*

Proof. We suppose that $\partial_2 D(z) = \{0 = \alpha_0 < \alpha_1 < \dots < \alpha_r < \alpha_{r+1} = 1\}$ and we restrict again to an interval $[\alpha_i, \alpha_{i+1}]$. So we can suppose $\partial_2 D(z) = \{0, 1\}$. Let $m = x'(0^+)$ and let $n \in \mathbb{N}$ such that $\sqrt[n]{m}$ is still an integral power of 2 (otherwise it does not make sense to look for a n -th root). We want to determine whether there is, or not, a $g \in \text{PL}_2(I)$ such that $g^{-1}xg = x$ and such that $g'(0^+) = \sqrt[n]{m}$. Suppose that there is such a g , then $g^{-k}xg^k = x$ and $(g^k)'(0^+) = m$. Then, by the uniqueness of the solution of the conjugacy problem with initial slope m (Corollary 4.1.31), we have that $g^n = x$. Conversely, if we have h such that $h^n = x$, then $h'(0^+) = \sqrt[n]{m}$. But $h^{-1}xh = h^{-1}h^n h = h^n = x$. Thus an element h is a n -th root of x if and only if it

is the solution the “differential type” equation with a given initial condition

$$\begin{cases} h^{-1}xh = x \\ h'(0^+) = \sqrt[n]{m}. \end{cases}$$

So we can decide whether or not there is a n -th root, by solving the equivalent conjugacy problem. Moreover, if the n -th root of g exists, it is computable by Theorem 4.1.35 and unique by Corollary 4.1.31. \square

Proposition 4.2.2 (Centralizers). *Suppose $x \in F$, then its centralizer is $C_F(x) \cong F^m \times \mathbb{Z}^n$, for some positive integers m, n such that $0 \leq m \leq n + 1$ (see figure 4.9).*

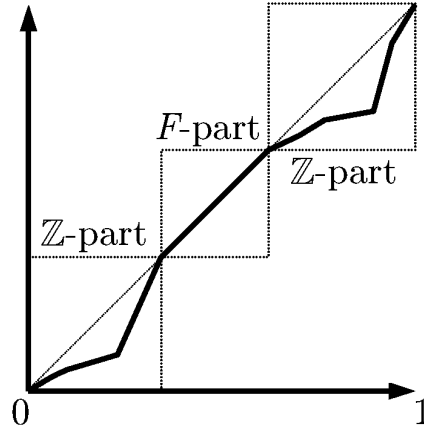


Figure 4.9: The structure of centralizers in F

Proof. Consider the conjugacy problem with $y = z = x$ and let $\partial_2 D(x) = \{\eta = \alpha_0 < \alpha_1 < \dots < \alpha_s < \alpha_{s+1} = \zeta\}$. Since all the points of $\partial_2 D(x)$ are fixed by x then $g \in C_{\text{PL}_2(I)}(x)$ must fix the set $\partial_2 D(x)$ and thus each of the α_i 's. This implies that we can restrict to solve the conjugacy problem in each of the subgroups $\text{PL}_2([\alpha_i, \alpha_{i+1}]) = \text{PL}_2^0([\alpha_i, \alpha_{i+1}])$ and so we can assume that $x \in \text{PL}_2^0(I)$. If $x = id$, then it is immediate $C_{\text{PL}_2(I)}(x) = \text{PL}_2(I)$. Suppose $x \neq id$ on $[0, 1]$, then the map

$\varphi_{x,x}$ of Corollary 4.1.31 is a non-trivial injective group homomorphism. Thus $C_{\text{PL}_2(I)}(x) \cong \log_2(\text{Im } \varphi_{x,x}) \leq \mathbb{Z}$, and so $C_{\text{PL}_2(I)}(x)$ is isomorphic to a subgroup of \mathbb{Z} . Therefore $C_{\text{PL}_2(I)}(x) \cong \mathbb{Z}$. Let $[\alpha_{i_1}, \alpha_{i_1+1}], \dots, [\alpha_{i_n}, \alpha_{i_n+1}]$ be the family of intervals such that $x|_{[\alpha_{i_j}, \alpha_{i_j+1}]} \neq id$, then the number of intervals where there restriction of x is trivial cannot be more than $n + 1$: x can be trivial only on the intervals $[\eta, \alpha_{i_1}], [\alpha_{i_1+1}, \alpha_{i_2}], \dots, [\alpha_{i_{n-1}+1}, \alpha_{i_n}], [\alpha_{i_n+1}, \zeta]$. \square

Corollary 4.2.3. *Suppose $x \in \text{PL}_2(I)$ is such that $C_{\text{PL}_2(I)}(x) \cong \mathbb{Z}$, then $C_{\text{PL}_2(I)}(x) = \langle \sqrt[k]{x} \rangle$, for some $k \in \mathbb{Z}$.*

Proof. Let $\varphi_{x,x}$ be as in Corollary 4.1.31, then $\log_2(\text{Im } \varphi_{x,x}) = M\mathbb{Z}$, for some $M \in \mathbb{Z}$. Let $2^n = \varphi_{x,x}(x)$ and let $\widehat{x} = \varphi_{x,x}^{-1}(2^M)$. Thus there is a $k \in \mathbb{Z}$ with $2^n = \varphi_{x,x}(x) = \varphi_{x,x}(\widehat{x}^k) = 2^{kM}$. This implies that $k = n/M$ and that $\widehat{x} = \sqrt[k]{x}$, since $\varphi_{x,x}$ is injective. Thus $C_{\text{PL}_2(I)}(x) = \langle \sqrt[k]{x} \rangle$. \square

Proposition 4.2.4 (Intersection of Centralizers). *Let $x_1, \dots, x_k \in \text{PL}_2(I)$ and define $C := C_{\text{PL}_2(I)}(x_1) \cap \dots \cap C_{\text{PL}_2(I)}(x_k)$. If the interval I is divided by the points in the union $\partial_2 D(x_1) \cup \dots \cup \partial_2 D(x_k)$ into the intervals J_i then*

$$C = C_{J_1} \cdot C_{J_2} \cdot \dots \cdot C_{J_r},$$

where $C_{J_i} := \{f \in C \mid f(t) = t, \forall t \notin J_i\} = C \cap \text{PL}_2(J_i)$. Moreover, each C_{J_i} is isomorphic to either \mathbb{Z} , or $\text{PL}_2(J_i)$ or the trivial group.

Proof. The set $\partial_2 D(x_i)$ is fixed by all elements in $C_{\text{PL}_2(I)}(x_i)$, therefore all elements in C fix the end points of the intervals J_i . The decomposition of C as $C_{J_1} \cdot \dots \cdot C_{J_r}$ follows from the observation:

Claim: Let J and J' be intervals such that $J' \subseteq J$. Then for any $x \in \text{PL}_2(J)$, such that $\partial_2 D(x)$ does not contain any points in the interior of J' we have the

restriction of

$$C_{\text{PL}_2(J)}(x) \cap \{g \in \text{PL}_2(J) \mid g(J') = J'\}$$

to the interval J' is either trivial in the case that x does not preserve the interval J' or $C_{\text{PL}_2(J')}(x)$ otherwise.

Proof of the Claim. Let $g \in C_{\text{PL}_2(J)}(x) \cap \{g \in \text{PL}_2(J) \mid g(J') = J'\}$. If $x(J') = J'$ then it is immediate that $g|_{J'} \in C_{\text{PL}_2(J')}(x)$. Suppose now that $x(J') \neq J'$ and $g|_{J'} \neq \text{id}$ and say that $J' = [\gamma_1, \gamma_2]$. Thus $x(\gamma_1) \neq \gamma_1$ or $x(\gamma_2) \neq \gamma_2$. Without loss of generality we can assume that $x(\gamma_1) \neq \gamma_1$. Let $[c, d]$ be the largest interval containing γ_1 such that $x(t) \neq t$ for any $t \in \mathbb{Z}[1/2] \cap (c, d)$. The proof of the previous Proposition implies that g coincides with $(\sqrt[k]{x})^k$ for some root of x and some integer k on the interval $[c, d]$. Since $\sqrt[k]{x}(\gamma_1) \neq \gamma_1$, k must be 0 and so g is the identity map on $[c, d]$. The restrictions on J' and J imply that $J' \subseteq [c, d]$, which completes the proof. \square

By the previous claim we see that, for each $i = 1, \dots, r$ and $j = 1, \dots, k$, the restriction of the subgroup $C_{\text{PL}_2(I)}(x_j) \cap \{g \in \text{PL}_2(I) \mid g(J_i) = J_i\}$ is either trivial or equal to $C_{\text{PL}_2(J_i)}(x_j)$. Thus $C_{J_i} = \text{id}$ or $C_{J_i} = C_{\text{PL}_2(J_i)}(x)$ for some $x \in \text{PL}_2(I)$ which, by the previous Proposition, is isomorphic with \mathbb{Z} or $\text{PL}_2(J_i)$ \square

Corollary 4.2.5. *The intersection of any number $k \geq 2$ centralizers of elements of F is equal to the intersection of 2 centralizers.*

Proof. We use the same notation of Proposition 4.2.4, where the x_i 's do not denote the standard generators of $\text{PL}_2(I)$ seen in Chapter 1, but only some arbitrary elements of the group. Let $C = C_{\text{PL}_2(I)}(x_1) \cap \dots \cap C_{\text{PL}_2(I)}(x_k)$ be the intersection of $k \geq 2$ centralizers of elements of F . By the previous Proposition we have $I = J_1 \cup \dots \cup J_r$ and $C = C_{J_1} \cdot \dots \cdot C_{J_r}$. We want to define $w_1, w_2 \in \text{PL}_2(I)$ such that $C = C_{\text{PL}_2(I)}(w_1) \cap C_{\text{PL}_2(I)}(w_2)$. We define them on each interval $J_i := [\alpha_i, \alpha_{i+1}]$,

depending on C_{J_i} . *Case 1:* If $C_{J_i} = id$, then we define w_1, w_2 as any two elements in $PL_2^<(J_i)$ such that are not one a power of another. *Case 2:* If $C_{J_i} \cong \langle x \rangle$ for some $id \neq x \in PL_2(J_i)$, then we define $w_1 = w_2 = x$. *Case 3:* If $C_{J_i} = PL_2(J_i)$, then we define $w_1 = w_2 = id$. \square

Question 4.2.6. Corollary 4.2.5 determines that any intersection of more than one centralizer of elements in F can be expressed as the intersection $C_F(w_1) \cap C_F(w_2)$ for two suitable elements $w_1, w_2 \in F$. Is it possible to build the two elements w_1, w_2 inside the subgroup $\langle x_1, \dots, x_k \rangle$? The current proof does not give an answer to this question.

4.3 The k -Simultaneous Conjugacy Problem in $PL_2(I)$

We will make a sequence of reductions to solve first a particular case. These reductions will use the fact that we are able to solve the ordinary conjugacy problem. First we notice that, since we know how to solve the ordinary conjugacy problem, then solving the $(k + 1)$ -simultaneous conjugacy problem is equivalent to find a positive answer to the following problem:

Problem 4.3.1. Is there an algorithm such that given (x_1, \dots, x_k, y) and (x_1, \dots, x_k, z) it can decide whether there is a function $g \in C_{PL_2(I)}(x_1) \cap \dots \cap C_{PL_2(I)}(x_k)$ such that $g^{-1}yg = z$?

Since we understand the structure of the intersection of centralizers, we are going to work on solving this last question. Our strategy now is to reduce the problem to the ordinary conjugacy problem and to isolate a very special case that must be dealt with.

4.3.1 General case: any k and any centralizer

This subsection deals with the general case. We will first extend Theorem 4.1.4 and then we will use our description for the intersection of many centralizers to solve the general problem. The argument of Proposition 4.3.3 will show us that we can build possible conjugators by using the stair algorithm and then check if they are in an intersection of centralizers. This will be verifiable, since we have given a description of such intersection in Proposition 4.2.4.

Lemma 4.3.2. *Let $x_1, \dots, x_k, y, z \in \text{PL}_2(J)$. We can determine whether there is, or not, a $g \in C = C_{\text{PL}_2(J)}(x_1) \cap \dots \cap C_{\text{PL}_2(J)}(x_k)$ such that $g(D(y)) = D(z)$.*

Proof. The proof is essentially the same as that of Corollary 4.1.8 on each of the intervals between two dyadic fixed points of y and z . The only new tool required is Lemma 4.1.33 on the intervals where C is isomorphic to \mathbb{Z} . We omit the details of this proof. \square

Proposition 4.3.3. *Let $x_1, \dots, x_k, y, z \in \text{PL}_2(J)$. We can determine whether there is, or not, a $g \in C = C_{\text{PL}_2(J)}(x_1) \cap \dots \cap C_{\text{PL}_2(J)}(x_k)$ with $g^{-1}yg = z$.*

Proof. Apply Lemma 4.3.2 to make $D(y) = D(z)$, if possible. Recall that a candidate conjugator must centralize x_1, \dots, x_k too, so it has to fix $\bigcup_{i=1}^k \partial_2 D(x_i)$ and $\partial_2 D(y) = \partial_2 D(z)$. Let $\bigcup_{i=1}^k \partial_2 D(x_i) = \{\lambda_m\}_m$ and $\partial_2 D(y) = \{\mu_1 < \dots < \mu_k\}$ and let J_i denote the interval $[\mu_i, \mu_{i+1}]$, for $i = 1, \dots, k-1$. We build g on each interval J_i , depending on how y is defined on J_i . We have the following three cases:

Case 1: y is the identity on J_i . In this case we define g to be the identity on J_i .

Case 2: y is not the identity on J_i and there is a point $\lambda_j \in \bigcup_{i=1}^k \partial_2 D(x_i)$ which is in the interior of J_i . Since $\mu_i < \lambda_j < \mu_{i+1}$ and λ_j is dyadic, then $\lambda_j \notin \partial_2 D(y)$ and

in particular λ_j is not fixed by y and z . Since $g(\lambda_j) = \lambda_j$, the proof of Lemma 4.1.15(ii) implies that $g'(\mu_i^+) = \lim_{n \rightarrow \infty} \frac{y^n(\lambda_j) - \mu_i}{z^n(\lambda_j) - \mu_i}$, hence the slope of g on the right of μ_i is uniquely determined. Therefore we can apply Proposition 4.1.32(iii) to build the unique candidate conjugator g .

Case 3: y is not the identity on J_i and $\bigcup_{i=1}^k \partial_2 D(x_i)$ does not contain any point of the interior of J_i . More precisely, each x_r does not fix any point in J_i and so, by the Claim contained in the proof of Proposition 4.2.4 we have that the restriction group

$$C_{\text{PL}_2(J)}(x_r) \cap \{g \in \text{PL}_2(J) \mid g(J_i) = J_i\}$$

is the trivial group or $\text{PL}_2(J_i)$ or isomorphic to a copy of \mathbb{Z} . Since C_{J_i} is the intersection of all the restriction groups for $r = 1, \dots, k$, then C_{J_i} will also be trivial or $\text{PL}_2(J_i)$ or infinite cyclic. If C_{J_i} is trivial, we choose g to be trivial on J_i . If $C_{J_i} = \text{PL}_2(J_i)$ then the construction reduces to solving the ordinary conjugacy problem in $\text{PL}_2(J_i)$. The case $C_{J_i} \cong \mathbb{Z}$ will be covered in Subsection 4.3.2.

Finally we have to verify that the element g constructed by the above procedure conjugates y to z and commutes with x . \square

The restatement of the k -simultaneous conjugacy problem given in Problem 4.3.1 and the previous Proposition imply the result of Theorem A in the introduction.

4.3.2 A special case: $k = 1$ and $C_{\text{PL}_+(J)}(x) \cong \mathbb{Z}$

This subsection is technical and it deals with a variant of the ordinary conjugacy problem. We want to see if we can solve it when we have a restriction on the possible conjugators. Thus, given x, y, z we want to see if $g^{-1}yg = z$ for a $g \in$

$C_{\text{PL}_2(J)}(x) \cong \mathbb{Z}$. In particular, if $\sqrt[m]{x}$ is the “smallest possible” root (in the sense of the proof of centralizers in $\text{PL}_2(J)$), then we need to find if there is a power of $\sqrt[m]{x}$ which conjugates y to z . Since $C_{\text{PL}_2(J)}(x) = C_{\text{PL}_2(J)}(\sqrt[m]{x}) = \langle \sqrt[m]{x} \rangle$ then we can substitute x with $\widehat{x} := \sqrt[m]{x}$. For simplicity, we assume still call \widehat{x} with x . The plan for this subsection will be to reduce to solve an equation of the type

$$f^k = wh^k$$

where f, h, w are given, $w'(\eta^+) = 1$ and we need to find if there is any $k \in \mathbb{Z}$ satisfying the previous equation. The second step will be to prove that there is only a finite number of k 's to that may solve the equation and so we try all of them.

We need first to run the usual conjugacy problem on $[\eta, \zeta]$ between y and z to see if they are conjugate. If they are, we continue. Otherwise we stop. Let $C_{\text{PL}_2(J)}(y, z) = \{g \in \text{PL}_2(J) \mid g^{-1}yg(t) = z(t), \text{ for all } t \in J\} = g_0 \cdot C_{\text{PL}_2(J)}(y)$, for some $g_0 \in T$. Now $C_{\text{PL}_2(J)}(y) \cong \mathbb{Z}^s \times \text{PL}_2(J)^t$. Notice that $s = t = 0$ is impossible.

If $s + t \geq 2$, then there must be some $\tau \in (\eta, \zeta) \cap \mathbb{Z}[\frac{1}{2}]$ fixed point for every element in $C_{\text{PL}_2(J)}(y)$. So if y and z are conjugate through a power of x then there is a k such that $x^k(\tau) = g_0(\tau)$. Notice $x(\tau) \neq \tau$, so we apply Lemma 4.1.33 with $\mu := g_0(\tau)$ and find, if possible a unique integer \bar{k} such that $x^{\bar{k}}(\tau) = \mu$. Now we take $g := x^{\bar{k}}$ and we check if it is a conjugator or not.

If $s = 0, t = 1$, then this would mean that $C_{\text{PL}_2(J)}(y) \cong \text{PL}_2(J)$ and so that $y = id$ on $[\eta, \zeta]$ and so do not need to check the powers of x , but simply if the function $z = id$ on $[\eta, \zeta]$.

If $s = 1, t = 0$, then $C_{\text{PL}_2(J)}(y) = \langle \widehat{y} \rangle \cong \mathbb{Z}$, for \widehat{y} a generator. Thus, y and z are

conjugate through an element of $C_{\text{PL}_2(J)}(x)$, if and only if there exist $k, m \in \mathbb{Z}$ such that $x^m = g_0 \widehat{y}^n$ in $[\eta, \zeta]$.

Lemma 4.3.4. *Let $x, y, z \in \text{PL}_2(J)$ such that $C_{\text{PL}_2(J)}(x) = \langle x \rangle$ and $C_{\text{PL}_2(J)}(y) = \langle \widehat{y} \rangle$. Then there exists $X, Y, G_0 \in \text{PL}_2(J)$ such that $G'_0(\eta^+) = 1$ and following two problems are equivalent:*

(i) *Find powers $k, m \in \mathbb{Z}$ such that $x^m = g_0 \widehat{y}^n$*

(ii) *Find a power $k \in \mathbb{Z}$ such that $X^k = G_0 Y^k$.*

Proof. Suppose we have $x'(\eta^+) = 2^\alpha, \widehat{y}'(\eta^+) = 2^\beta, g'_0(\eta^+) = 2^\gamma$ for some $\alpha, \beta, \gamma \in \mathbb{Z}$, then we must have $2^{\alpha m} = (x^m)'(\eta^+) = (g_0 \widehat{y}^n)'(\eta^+) = 2^{\gamma + \beta n}$ and so $\alpha m = \gamma + \beta n$. Thus, in order for y and z to be conjugate we must have that $\gcd(\alpha, \beta)$ divides γ . That is, $\gamma = \alpha m_0 - \beta n_0$, for some $m_0, n_0 \in \mathbb{Z}$ which can be computed and thus $\alpha(m - m_0) = \beta(n - n_0)$. We can change variables and call $\widetilde{m} = m - m_0$ and $\widetilde{n} = n - n_0$. So we have to find $\widetilde{m}, \widetilde{n}$ such that $\alpha \widetilde{m} = \beta \widetilde{n}$ and so that

$$\frac{\alpha}{\gcd(\alpha, \beta)} \widetilde{m} = \frac{\beta}{\gcd(\alpha, \beta)} \widetilde{n}$$

Thus there must exist a $k \in \mathbb{Z}$ such that

$$\widetilde{m} = \frac{\beta}{\gcd(\alpha, \beta)} k \quad \text{and} \quad \widetilde{n} = \frac{\alpha}{\gcd(\alpha, \beta)} k.$$

Going backwards, we write

$$m := \frac{\beta}{\gcd(\alpha, \beta)} k + m_0 \quad \text{and} \quad n := \frac{\alpha}{\gcd(\alpha, \beta)} k + n_0.$$

By substituting these two values in the equation $x^m = g_0 \widehat{y}^n$ we get

$$(x^{\frac{\beta}{\gcd(\alpha, \beta)}})^k = x^{-m_0} g_0 \widehat{y}^{n_0} (\widehat{y}^{\frac{\alpha}{\gcd(\alpha, \beta)}})^k$$

We rename $X = x^{\frac{\beta}{\gcd(\alpha, \beta)}}$, $G_0 = x^{-m_0} g_0 \widehat{y}^{n_0}$ and $Y = \widehat{y}^{\frac{\alpha}{\gcd(\alpha, \beta)}}$ and so we are left to find a $k \in \mathbb{Z}$, if it exists, such that

$$X^k = G_0 Y^k. \tag{4.3}$$

Notice that, with these adjustments, $G_0(\eta^+) = 2^0 = 1$. \square

In the last case we are examining, both x and y cannot have fixed dyadic points, since their centralizers are cyclic groups. Thus $D(x) \cap (\eta, \zeta)$ and $D(y) \cap (\eta, \zeta)$ must be empty or finite. The same is also true for the new functions X and Y , i.e. $D(X) \cap (\eta, \zeta)$ and $D(Y) \cap (\eta, \zeta)$ must be empty or finite. For sake of simplicity, we will still call X, Y, G_0 with lowercase letters. We will make distinction in the following cases, by checking what are $D(x) \cap (\eta, \zeta)$ and $D(y) \cap (\eta, \zeta)$ and see if they coincide or not.

$D(x) \cap (\eta, \zeta) \neq D(y) \cap (\eta, \zeta)$. There exists a $\tau \in (\eta, \zeta)$ with $y(\tau) = \tau \neq x(\tau)$. Thus, by applying Lemma 4.1.33, we can determine if there is a k such that $x^k(\tau) = g_0(\tau)$. We act similarly if there is a $\tau \in (\eta, \zeta)$ with $x(\tau) = \tau \neq y(\tau)$.

$D(x) \cap (\eta, \zeta) = D(y) \cap (\eta, \zeta) \neq \emptyset$. Suppose $D(x) = D(y) = \{r_1 < \dots < r_v\}$. Observe that if the equation has a solution then $g_0(r_i) = r_i$ for all r_i . If these conditions are satisfied, then we can build all the solutions by solving the equation in each interval $[r_i, r_{i+1}]$. This reduces the problem to the next case.

$D(x) \cap (\eta, \zeta) = D(y) \cap (\eta, \zeta) = \emptyset$, that is we have that $x, y \in \text{PL}_2^<(J) \cup \text{PL}_2^>(J)$. We can now assume that both $x, y \in \text{PL}_2^<(J)$. Define

$$K := \{k \in \mathbb{Z} \text{ such that } x^k(t) = g_0(y^k(t)) \text{ for all } t \in J\}.$$

Our goal is to find whether or not $K \neq \emptyset$. The first step will be to prove that the set K is finite, by computing directly its upper and lower bounds. Therefore, we will have that $K \subseteq \mathbb{Z} \cap [l_0, k_0]$, for some integers l_0, k_0 , and so we can check all these integers and see if any satisfies $x^k(t) = g_0(y^k(t))$.

Lemma 4.3.5. *Let $x, y \in \text{PL}_2^{\leq}(J)$ and let $K := \{k \in \mathbb{Z} \text{ such that } x^k = g_0 y^k\}$, then K is bounded.*

Proof. The first step is to prove that there exists a $k_0 \in \mathbb{Z}$, upper bound for K . Suppose that K has no upper bound. Let $\theta < \zeta$ be a point such that $g_0(t) = t$ and $x(t) = y(t)$ on $[\eta, \theta]$. Let $\psi > \theta$ a number such that $x(\psi) < y(\psi)$ and $x(t) \leq y(t)$ for $t \leq \psi$. Since $y \in \text{PL}_2^{\leq}(J)$ then $\lim_{k \rightarrow \infty} y^k(\psi) = \eta$, and so we can choose a $k_0 \in K$ be a large enough number such that $y^{k_0}(\psi) < \theta$. Suppose $k \geq k_0$, by definition of θ and $k_0 \in K$ we have

$$x^k(\psi) = g_0(y^k(\psi)) = y^k(\psi).$$

Now recall that $x(\psi) < y(\psi) < \theta + \varepsilon$ and so, since $x \leq y$ on $[\eta, \psi]$

$$\begin{aligned} x^k(\psi) &= x^{k-1}(x(\psi)) < x^{k-1}(y(\psi)) \\ &= x^{k-2}(x(y(\psi))) \leq x^{k-2}(y^2(\theta + \varepsilon)) \\ &\leq \dots \leq x(y^{k-1}(\psi)) \leq y^k(\psi). \end{aligned}$$

By comparing the last two expressions, we get $x^k(\psi) < y^k(\psi) = x^k(\psi)$. Contradiction. Therefore k_0 is an upper bound for K .

We now want to bound the K from below, and so we use a similar technique. If $k \in K$ is negative, then we consider the equation

$$y^{-k} = x^{-k} g_0 = g_0(g_0^{-1} x^{-k} g_0) = g_0(g_0^{-1} x g_0)^{-k} = g_0 \widehat{x}^{-k}$$

where we have set $\widehat{x} := g_0^{-1} x g_0$. Since $D(x) = \emptyset$, then $D(\widehat{x}) = \emptyset$ and $\widehat{x} \in \text{PL}_2^{\leq}(I)$. So we have reduced to the situation of the previous claim (with \widehat{x} and y switched in their role) and we obtain that the set of possible $(-k)$'s is bounded above, so that k is bounded below. \square

Since K is finite the k 's to be checked are finite and we can find its bound in finite time. Now we can check all possible the elements of K and we conclude this case.

4.3.3 The twisted conjugacy problem for $\text{PL}_2(I)$

We conclude this section by describing an interesting open question for Thompson's group F . It has been shown by Bogopolski, Martino, Maslakova and Ventura [11] and [12] that the conjugacy problem for certain extensions of groups can be reduced to solving the twisted conjugacy problem for a subgroup. We say that a group G has *solvable φ -twisted conjugacy problem*, for a given $\varphi \in \text{Aut}(G)$, if there is an algorithm such that, given any two elements $y, z \in G$, we can determine whether there is, or not, a $g \in G$ such that $\varphi(g)^{-1}yg = z$. Brin [14] has classified the structure of automorphisms of Thompson's group F . Let $\text{PL}_{dis}(\mathbb{R})$ denote the group of piecewise-linear orientation-preserving homeomorphisms with finitely many breakpoints occurring at dyadic rational coordinates, such that every slope is an integral power of 2 and with a discrete set of breakpoints (infinitely many breakpoints are possible): then F is isomorphic to the subgroup H of $\text{PL}_{dis}(\mathbb{R})$ of elements f such that there is an interval $[a_f, b_f]$ and $f(t) = t + m_f$ on (b_f, ∞) and $f(t) = t + k_f$ on $(-\infty, a_f)$, for some integers m_f, k_f . Then any orientation-preserving automorphism of H is given by the maps $\varphi : H \rightarrow H$, defined by $\varphi(g) = \tau^{-1}g\tau$ where $\tau \in A$, the subgroup of $\text{PL}_{dis}(\mathbb{R})$ such that there is an interval $[m_\tau, n_\tau]$ with $\tau(t+1) = \tau(t) + 1$ for any $t \notin [m_\tau, n_\tau]$. Hence, if we rewrite the φ -twisted conjugacy problem for Thompson's group F seen as the subgroup H we can rewrite it as

$$z = \varphi(g)^{-1}yg = \tau^{-1}g^{-1}\tau yg$$

and so it becomes

$$g^{-1}(\tau y)g = \tau z$$

that is, a conjugacy problem for the elements $\tau y, \tau z \in A$ with respect to an element $g \in F$. It is an interesting problem to work on solving this generalization of the conjugacy problem and see if any of the presented techniques of closed diagrams, Mather invariants or the Stair Algorithm can be extended to this setting.

Question 4.3.6. Is the twisted conjugacy problem solvable for the group F ?

4.4 Stair Algorithm in $\text{PL}_{S,G}(I)$

We now move on to prove the solvability of the simultaneous conjugacy problem to other subgroups of $\text{PL}_+(I)$ whose structure generalizes that of Thompson's group F . We remark that Brin and Squier [19] give a criterion for conjugacy in $\text{PL}_+(I)$. Let S be a subring of \mathbb{R} , let $U(S)$ be the group of invertible elements of S and let G be a subgroup of $U(S) \cap \mathbb{R}_+$. For any subinterval J of I , we define $\text{PL}_{S,G}(J)$ to be the group of piecewise linear orientation-preserving homeomorphism from the interval J into itself, with only a finite number of breakpoints and such that

- all breakpoints are in the subring S ,
- all slopes are in the subgroup G ,

the product of two elements is given by the composition of functions. If $G = U(S) \cap \mathbb{R}_+$ we write $\text{PL}_S(J)$ instead of $\text{PL}_{S,G}(I)$. Thompson's group F can

thus be recovered as the group $\text{PL}_{\mathbb{Z}[\frac{1}{2}], \langle 2 \rangle}(I)$. We observe that, in order to make some calculations possible inside the ring S and its quotients, we need to ask for some requirements to be satisfied by S from the computability standpoint. These assumptions will be clearly stated in Remark 4.4.7 and will be assumed throughout the remainder of the chapter.

We introduce briefly the notation to generalize the results obtained on F . For a subset $J \subseteq [0, 1]$, we denote with ∂J the usual boundary of J in $[0, 1]$. For an interval $J = [\eta, \zeta] \subseteq I$ such that $\partial J \subseteq S$, a function $f \in \text{PL}_{S,G}(J)$ can be extended to the interval I by $f(t) = t$ for $t \in I \setminus J$, which allows us to consider $\text{PL}_{S,G}(J)$ as a subgroup of $\text{PL}_{S,G}(I)$. For a function $f \in \text{PL}_{S,G}(J)$ we define

$$D_J(f) := \{t \in J \mid f(t) = t\},$$

to simplify the notation will often drop the subscript J .

Definition 4.4.1. We define $\text{PL}_{S,G}^<(J)$ (and respectively. $\text{PL}_{S,G}^>(J)$) to be the set of all functions in $\text{PL}_{S,G}(J)$ with graph below the diagonal (respectively, above the diagonal).

Given a function $f \in \text{PL}_{S,G}(I)$ and a number $0 < t_0 < 1$ fixed by f , it is not always true that $t_0 \in S$. For any subset $J \subseteq I$ we define

$$\partial_S J := \partial J \cap S$$

Definition 4.4.2. We define $\text{PL}_{S,G}^0(J) \subseteq \text{PL}_{S,G}(J)$, the set of functions $f \in \text{PL}_{S,G}(J)$ such that the set $D(f)$ does not contain elements of S other than the endpoints of J , i.e., $D(f)$ is discrete and $\partial_S D(f) = \partial_S J$.

Question 4.4.3. Given two elements $\alpha, \beta \in S$, is it true that there is a $g \in \text{PL}_{S,G}(J)$ such that $g(\alpha) = \beta$? We will now discuss conditions to verify this generalization of Proposition 3.2.3 and of Corollary 4.1.7.

Definition 4.4.4. We define an ideal in S given by $\mathcal{I}_{S,G} = \langle (g - 1) \mid g \in G \rangle$. We denote with $\pi_{S,G} : S \rightarrow S/\mathcal{I}$ the natural quotient map. Unless otherwise stated, we will drop the subscript and write \mathcal{I} and π instead of $\mathcal{I}_{S,G}$ and $\pi_{S,G}$.

The following two results are used to detect when two points of S are in the same $\text{PL}_{S,G}$ -orbit.

Lemma 4.4.5. *Let $J \subseteq [0, 1]$ be a closed interval with at least one of the endpoints η in S and let $g \in \text{PL}_{S,G}(J)$. Then, for every $t \in J \cap S$, we have $\pi(g(t)) = \pi(t)$.*

Proof. We can assume that the η is the left one and we apply induction on the number of breakpoints before t . In case the endpoint in S is the right one, we apply induction on the breakpoints after t . Let $\{\eta_1, \dots, \eta_r\}$ be the set of all breakpoints of g on the interval $[\eta, t)$. Then $g(t) = c_r(t - \eta_r) + g(\eta_r)$ for some suitable $c_i \in G$. By induction on r we have that $\pi(g(\eta_r)) = \pi(\eta_r)$ and thus

$$\begin{aligned} \pi(g(t)) &= \pi(c_r(t - \eta_r) + g(\eta_r)) = \\ \pi(c_r - 1)\pi(t - \eta_r) + \pi(1)\pi(t - \eta_r) + \pi(g(\eta_r)) &= \\ \pi(t - \eta_r) + \pi(\eta_r) &= \pi(t). \square \end{aligned}$$

This result gives us a necessary condition on how homeomorphisms can be built. We want to know what orbits of elements are under the action of $\text{PL}_{S,G}(J)$.

Proposition 4.4.6. *Let $J \subseteq [0, 1]$ be a closed interval with both endpoints in S and let $u, v \in J \cap S$. Then $\pi(u) = \pi(v)$ if and only if there is a $g \in \text{PL}_{S,G}(J)$ such that $g(u) = v$.*

The proof of this proposition can be found in the Appendix (see Proposition A.2.1).

Remark 4.4.7 (Computational Requirements). We need to add a few requirements to the ring S in order to make a machine able to work with the algorithm. It is reasonable to make the following assumptions to work in the ring S :

- There is solution to the membership problem in S (*i.e.* an algorithm to determine whether an element $s \in \mathbb{R}$ lies in S or not)
- There is a solution to the membership problem in \mathcal{I}
- There is an algorithm that, for every $q \in S$, is able to determine whether two elements in the quotient ring $S/q\mathcal{I}$ are equal or not.
- There is an algorithm such that, given $a, b, c \in G$, it is able to determine whether or not there exist $x, z \in \mathbb{Z}$ such that $a^x = bc^z$.

All these requirements are reasonable to assume in order to make computations inside S and will be checkable in the special cases that we take as examples in Section 4.6.

Remark 4.4.8. By taking logarithms, we can rewrite all of the terms of the last requirement on the algorithm in base b , so that it becomes equivalent to the following: given any $\alpha, \beta, \gamma \in \mathbb{R}$, determine whether or not they are linearly dependent over \mathbb{Q} and, if they are, we can find $q_1, q_2 \in \mathbb{Q}$ such that $\gamma = q_1\alpha + q_2\beta$. This rewriting transforms the equation $a^x = b^y c^z$ into a \mathbb{Q} -linearity dependence relation, hence if there is a solution, it is unique.

Remark 4.4.9. In general, given two intervals J_1, J_2 with endpoints in S , the groups $\text{PL}_{S,G}(J_1)$ and $\text{PL}_{S,G}(J_2)$ may not be isomorphic (that is, the analogue of Theorem 1.1.5 may not hold). Proposition 4.4.6 tells us that two elements in S are in the same $\text{PL}_{S,G}$ -orbit if their image under the map π is the same. For example in the cases $S = \mathbb{R}, G = \mathbb{R}_+$ and $S = \mathbb{Q}, G = \mathbb{Q}^*$ and $S = \mathbb{Z}[\frac{1}{2}], G = \langle 2 \rangle$, it is

not difficult to see that every two points in S have the same image under π and that any two groups $\text{PL}_{S,G}(J_1)$ and $\text{PL}_{S,G}(J_2)$ are thus isomorphic, for any two intervals J_1, J_2 with endpoints in S . On the other hand, if we consider generalized Thompson's groups (see Section 4.6), it can be shown that the number of orbits is finite but more than one, so that there are only finitely many isomorphism classes for the groups $\text{PL}_{S,G}(J)$, for $S = \mathbb{Z}[\frac{1}{n_1}, \dots, \frac{1}{n_k}]$ and $G = \langle n_1, \dots, n_k \rangle$ for $n_1, \dots, n_k \in \mathbb{Z}$. In general, it seems likely that if two elements $\alpha, \beta \in S$ have different image under π then the groups $\text{PL}_{S,G}([0, \alpha])$ and $\text{PL}_{S,G}([0, \beta])$ are not isomorphic, but it is not easy to prove it.

4.4.1 Making $D(y)$ and $D(z)$ coincide

We start by generalizing Proposition 4.4.6 to a finite number of points.

Lemma 4.4.10. *Let $J = [\eta, \zeta] \subseteq [0, 1]$ be a closed interval with endpoints in S and suppose we have $u_1, v_1, \dots, u_k, v_k \in J \cap S$ such that $\pi(u_i) = \pi(v_i)$ for all $i = 1, \dots, k$. Then there exists a $g \in \text{PL}_{S,G}(J)$ such that $g(u_i) = v_i$ for all $i = 1, \dots, k$.*

Proof. We can assume that $J = [\eta, \zeta]$ and that the u_i 's are ordered in an increasing sequence $u_1 < \dots < u_k$ and therefore $v_1 < \dots < v_k$. By Proposition 4.4.6, there is an $g_1 \in \text{PL}_{S,G}(J)$ such that $g_1(u_1) = v_1$. Now we notice that $v_1 = g_1(u_1) < g_1(u_2) < \dots < g_1(u_k)$ and so we restrict to the interval $[v_1, \zeta]$ and, since $\pi(g_1(u_2)) = \pi(u_2) = \pi(v_2)$ we can use again Proposition 4.4.6 to find an $h_2 \in \text{PL}_{S,G}([v_1, \zeta])$ such that $h_2(g_1(u_2)) = v_2$. Define

$$g_2(t) := \begin{cases} t & t \in [\eta, v_1] \\ h_2(t) & t \in [v_1, \zeta] \end{cases}$$

so that $g_2g_1(u_1) = v_1, g_2g_1(u_2) = v_2$ and $g_2 \in \text{PL}_{S,G}(J)$. By iterating this procedure, we build functions $g_i \in \text{PL}_{S,G}(J)$ such that $g_i g_{i-1} \dots g_1(u_j) = v_j$ for all $j = 1, \dots, i$ and $i = 1, \dots, k$. Thus we define $g := g_k g_{k-1} \dots g_1 \in \text{PL}_{S,G}(J)$ and we get a function such that $g(u_i) = v_i$. \square

The previous Lemma yields the following natural generalization of the Extension Lemma 4.1.5 which we state without proof.

Lemma 4.4.11 (Extension of Partial Maps). *Let $J \subseteq [0, 1]$ be a closed interval with endpoints in S and suppose $I_1, \dots, I_k \subseteq J$ is a finite family of disjoint closed intervals in increasing order and of the form $I_i = [a_i, b_i]$, for all $i = 1, \dots, k$ and $a_i, b_i \in S$. Let $J_1, \dots, J_k \subseteq J$, with $J_i = [c_i, d_i]$, be another family of intervals with the same property and such that $\pi(a_i) = \pi(c_i)$ and $\pi(b_i) = \pi(d_i)$. Suppose that $g_i : I_i \rightarrow J_i$ is a piecewise-linear function with a finite number of breakpoints, occurring at points in S and with slopes in G . Then there exists a $\tilde{g} \in \text{PL}_{S,G}(J)$ such that $\tilde{g}|_{I_i} = g_i$. \square*

Let $g \in \text{PL}_{S,G}(J)$ be equal to $g(t) = at + b$ around a point $q \in \mathbb{R}$ fixed by f , for some $a \in G, b \in S$, then $q = b/(1 - a)$ and so the intersection points of f with the diagonal lie in Q_S , the field of fractions of S . Now that we have a way to recognize whether we can make two elements of S coincide through an element of $\text{PL}_{S,G}(J)$, we need to see if it is possible to do the same for the field of fractions Q_S .

Proposition 4.4.12. *Let $J = [\eta, \zeta] \subseteq [0, 1]$ be a closed interval with endpoints in S and let $\alpha, \beta \in J \cap Q_S$. There is a $g \in \text{PL}_{S,G}(J)$ with $g(\alpha) = \beta$ if and only if we can find $p, q, r \in S$ such that $\alpha = p/q, \beta = r/q$ and*

$$pG = rG \pmod{qI}$$

where qI denotes the product of the ideal generated by q and I .

Proof. Suppose there is a map $g \in \text{PL}_{S,G}(J)$ with $g(\alpha) = \beta$ and let $g(t) = ct + d$ in a small neighborhood J_α of α . We can choose representatives $p, q, r \in S$ such that $\alpha = p/q, \beta = r/q$ and then, since $g \in \text{PL}_{S,G}(J)$, we use Lemma 4.4.5 to get

$$\pi(t) = \pi(g(t)) = \pi(c - 1)\pi(t) + \pi(t) + \pi(d)$$

for all $t \in J_\alpha \cap S$ and therefore $\pi(d) = 0$, which implies $d \in I$. Conversely, suppose that we can write $\alpha = p/q, \beta = r/q$, for some $p, q, r \in S$ and that $pG = rG \pmod{qI}$. The second condition implies that there exist $c_1, c_2 \in G, d_2 \in I$ such that

$$c_1 r = c_2 p + q d_2$$

and so if we set $c = c_2/c_1$ and $d = d_2/c_1$, we get $r = cp + qd$. Let $f(t) = ct + d$ be a line through the point (α, β) and let $[\gamma, \delta] \subseteq J$ be a small interval such that $\gamma, \delta \in S$. Finding the interval $[\gamma, \delta]$ can be accomplished this way: we can assume $G \neq 1$ and pick any $1 \neq c \in G$ such that $0 < c < 1$. Then we choose $m, n \in \mathbb{N}$ such that $\eta + c^m < \alpha < \eta + nc^m < \zeta$ and we set $\gamma := \eta + c^m, \delta := \eta + nc^m$. Since $\pi(d) = 0$ we have that $\pi(f(\gamma)) = \pi(\gamma)$ and $\pi(f(\delta)) = \pi(\delta)$ and so, by the Extension Lemma 4.4.11 there is an $g \in \text{PL}_{S,G}(J)$ with $g|_{[\gamma, \delta]} = f$. By construction $g(\alpha) = \beta$ as required. \square

In a similar fashion, we can get the same result for a finite number of points. This amounts to finding small segments passing through the rational pairs (α_i, β_i) and then applying the Extension Lemma to obtain a homeomorphism of the whole interval J . We thus state without proof the following Lemma.

Lemma 4.4.13. *Let $J = [\eta, \zeta] \subseteq [0, 1]$ be a closed interval with endpoints in S and let $\alpha_i, \beta_i \in J \cap Q_S$ for $i = 1, \dots, k$. There is a $g \in \text{PL}_{S,G}(J)$ with $g(\alpha_i) = \beta_i$ if and only if there exist $g_1, \dots, g_k \in \text{PL}_{S,G}(J)$ such that $g_i(\alpha_i) = \beta_i$.*

By the assumptions made in Remark 4.4.7, we can detect whether or not two elements in Q_S are equal, thus we obtain the following generalizations of Corollary 4.1.8 and Lemma 4.1.4:

Corollary 4.4.14. *Let $J = [\eta, \zeta] \subseteq [0, 1]$ be a closed interval with endpoints in S and let $\alpha_i, \beta_i \in J \cap Q_S$ for $i = 1, \dots, k$. We can determine whether there is or not an $f \in \text{PL}_{S,G}(J)$ such that $g(\alpha_i) = \beta_i$ for every $i = 1, \dots, k$. \square*

Proposition 4.4.15. *Given $y, z \in \text{PL}_{S,G}(I)$, we can determine whether there is or not a $g \in \text{PL}_{S,G}(I)$ such that $g(D(y)) = D(g^{-1}yg) = D(z)$. If such a g exists, we can construct it. \square*

4.4.2 Linearity Boxes and Stair Algorithm

In this Subsection we generalize the results of Subsections 4.1.2, 4.1.3 and 4.1.5. First we observe that two conjugate elements y, z in $\text{PL}_{S,G}(I)$ must have the same slopes around the two endpoints, then we build an algorithm which makes these two elements coincide in a sequence of steps. More precisely, we build a sequence of functions g_1, g_2, \dots, g_k and of intervals $J_1 \subseteq J_2 \subseteq \dots \subseteq J_i \subseteq \dots$ such that $0 \in J_1$ and $g_i^{-1} \dots g_1^{-1}yg_1 \dots g_i = z$ on J_i . We prove that the procedure will stop because the two elements y, z coincide around the second endpoint of I . When the algorithm stops, we have that $J_k = [0, 1]$.

Lemma 4.4.16 (Linearity Boxes). *Suppose $y, z, g \in \text{PL}_{S,G}(J)$ and $g^{-1}yg = z$.*

(i) *If there exist two numbers $\alpha > 0$ and $c \geq 1$ such that $y(t) = z(t) = c(t - \eta) + \eta$ for $t \in [\eta, \eta + \alpha]$, then the graph of g is linear inside the square $[\eta, \eta + \alpha] \times [\eta, \eta + \alpha]$*

(ii) If there exist $\beta, c \in (0, 1)$ such that $y(t) = z(t) = c \cdot (t - \zeta) + \zeta$ on $[\beta, \zeta]$, then the graph of g is linear inside the square $[\beta, \zeta] \times [\beta, \zeta]$.

Proof. These results follow from the proofs of Lemma 4.1.10 and Remark 4.1.11.

□

We recall that $\text{PL}_{S,G}^0(J)$ denotes the set of functions $f \in \text{PL}_{S,G}(J)$ such that the set $D(f)$ does not contain elements of S other than the endpoints of J .

Proposition 4.4.17 (Stair Algorithm for $\text{PL}_{S,G}^0(J)$). *Let $J \subseteq [0, 1]$ be a closed interval with endpoints in S , let $y, z \in \text{PL}_{S,G}^0(J)$ such that $D(y) = D(z)$ and define $C_{\text{PL}_{S,G}(J)}(y, z) = \{g \in \text{PL}_{S,G}(J) | y^g = z\}$ the set of all conjugators. For any $\tau \in D(y)$ we define the map*

$$\begin{aligned} \varphi_{y,z,\tau} : C_{\text{PL}_{S,G}(J)}(y, z) &\longrightarrow \mathbb{R}_+ \\ g &\longmapsto g'(\tau), \end{aligned}$$

where if τ is an endpoint of J we take only a one-sided derivative. Then

(i) $\varphi_{y,z,\tau}$ is an injective map. In particular, if we define $\varphi_{z,\tau} := \varphi_{z,z,\tau}$, then $\varphi_{z,\tau}$ is a group homomorphism.

(ii) If $q \in G$ is a fixed number we can decide whether or not there is a $g \in \text{PL}_{S,G}(J)$ with initial slope $g'(\eta^+) = q$ such that $y^g = z$. If g exists, it is unique. In other words, if there is a g such that $\varphi_{y,z,\tau}(g) = \mu \in G$ then g is unique and can be constructed.

Proof. Immediate generalization of Corollary 4.1.31. □

Corollary 4.4.18. *Let $y, z \in \text{PL}_{S,G}^<(J)$ and $g \in \text{PL}_+(J)$ such that $y^g = z$ and $g'(\eta) \in G$. Then $g \in \text{PL}_{S,G}(J)$.*

4.4.3 Centralizers and Roots in $\text{PL}_{S,G}(J)$

This section proves a generalization of Proposition 4.2.2. The centralizers $C_{\text{PL}_{S,G}(J)}(z)$ of elements will be direct products of copies of \mathbb{Z} 's and of $\text{PL}_{S,G}(U)$'s, for some suitable intervals U . In order to prove this, we will use the Stair Algorithm to build a “section” of the map φ_x . As in the proof of Proposition 4.2.2, we will reduce the study to functions in $\text{PL}_{S,G}^0(J)$. Consider the conjugacy problem with $y = z$ and let $\partial_S D(z) = \{0 = \alpha_0 < \alpha_1 < \dots < \alpha_s < \alpha_{s+1} = 1\}$. Since all the points of $\partial_S D(z)$ are fixed by z , then $g \in C_{\text{PL}_{S,G}(J)}(z)$ must fix the set $\partial_S D(z)$ and thus each of the α_i 's. This implies that we can restrict to solving the conjugacy problem in each of the subgroups $\text{PL}_{S,G}([\alpha_i, \alpha_{i+1}]) = \text{PL}_{S,G}^0([\alpha_i, \alpha_{i+1}])$. If $z = 1$, it is immediate that $C_{\text{PL}_{S,G}(J)}(x) = \text{PL}_{S,G}(J)$, so now we can focus on $1 \neq z \in \text{PL}_{S,G}^0(J)$. Consider \mathbb{R}_+ to be the multiplicative group of positive real numbers. Let $A \subset \mathbb{R}_+$ be the set of all possible initial slopes of functions g such that $g^{-1}zg = z$. The set A is not empty, since $\langle z \rangle \subseteq C_{\text{PL}_{S,G}(J)}(z)$. For a given closed interval J with endpoints in S we define a map

$$\begin{aligned} \psi : A &\rightarrow C_{\text{PL}_{S,G}(J)}(z) \\ \alpha &\mapsto g_\alpha \end{aligned}$$

which sends an initial slope α to its associated conjugating function g_α . By the uniqueness of a conjugator with a given initial slope, we notice immediately that $g_\alpha \circ g_\beta = g_{\alpha\beta}$ and so A is a subgroup of \mathbb{R}_+ and ψ is a homomorphism of groups. Moreover, the uniqueness of the conjugator implies also that ψ is an isomorphism. The main result of this section is the following:

Theorem 4.4.19. *Let $J \subseteq [0, 1]$ be a closed interval with endpoints in S and let $id \neq z \in \text{PL}_{S,G}^0(J)$. Then $C_{\text{PL}_{S,G}(J)}(z)$ is isomorphic with \mathbb{Z} .*

Proof of Theorem 4.4.19. By the discussion above we have that the group $A =$

$\{g'(\eta^+) \mid g \in C_{\text{PL}_{S,G}(J)}(z)\}$ is isomorphic with $C_{\text{PL}_{S,G}(J)}(z)$. We start by assuming that $z \in \text{PL}_{S,G}^<(J)$ and we want to prove that A is discrete. We assume, by contradiction that A is not discrete.

Step 1: If A is not discrete, then A is dense in \mathbb{R}_+ .

Proof. This is a standard well known fact (for example see [54]). \square

Step 2: Let $[\eta, \alpha]^2$ be the first initial linearity box and $[\beta, \tau]^2$ be the first final linearity box, for some $\tau \leq \zeta$ fixed point for z . Without loss of generality, we can assume that the restriction $z|_{[\eta, \tau]} \in \text{PL}_+^<([\eta, \tau])$. Let r be a positive integer big enough so that $z^{-r}(\alpha) > \beta$. Then z^r is linear on $[\beta, z^{-r}(\alpha)]$, say with slope b .

Proof. Since A is dense in \mathbb{R}_+ , we can pick a $c \in C_{\text{PL}_{S,G}(J)}(z)$ such that $c'(\eta^+) < 1$ is arbitrarily close to 1. Now, observe that $c \in \text{PL}_+^<([\eta, \tau])$ and look at the two hand sides of $cz^r = z^rc$, by restricting this equality to the interval $[\beta, z^{-r}(\alpha)]$. Suppose $\{\mu_1 < \dots < \mu_k\}$ are the breakpoints of z^r on $[\beta, z^{-r}(\alpha)]$, hence they are also the breakpoints of cz^r on $[\beta, z^{-r}(\alpha)]$, since c is linear on $[\eta, \alpha]$. On the interval $[\beta, \tau]$ we can write $c^{-1}(t) = \lambda(t - 1) + 1$, where $\lambda = c'(\tau^-)$: if we have chosen $c'(\eta^+) \neq 1$ to be close enough to 1, then $\lambda < 1$ is also arbitrarily close to 1. Since c^{-1} is linear on $[\beta, \tau]$ then, if we choose λ close enough to 1, the set of breakpoints of z^rc on $[\beta, z^{-r}(\alpha)]$ will be $c^{-1}(\{\mu_1, \dots, \mu_k\}) = \{\lambda(\mu_1 - 1) + 1, \dots, \lambda(\mu_k - 1) + 1\}$. As $cz^r = z^rc$ on $[\beta, z^{-r}(\alpha)]$ we must have that $\{\mu_1, \dots, \mu_k\} = c^{-1}(\{\mu_1, \dots, \mu_k\})$ and so $\lambda = 1$, which is a contradiction. \square

Step 3: Define $a = \left. \frac{d}{dt} z^r(t) \right|_{t=\eta^+} < 1$ to be the initial slope of z^r . For every positive integer i , the map z^r is linear on $[z^{-ir}(\beta), z^{-(i+1)r}(\alpha)]$ with slope a .

Proof. We assume by induction that the result is true for any integer less than i .

Consider now the map $z^{(i+1)r}$ and apply the chain rule on two intervals, recalling that $\frac{d}{dt}z^r(t) = a$ on the intervals $[z^{-jr}(\beta), z^{-(j+1)r}(\alpha)]$ for any $j < i$:

$$\frac{d}{dt}z^{(i+1)r}(t) = a^i b \quad t \in [\beta, z^{-ir}(\alpha)]$$

$$\frac{d}{dt}z^{(i+1)r}(t) = a^{i-1} b \frac{d}{dt}z^r(t) \quad t \in [z^{-ir}(\beta), z^{-(i+1)r}(\alpha)].$$

We apply Step 2 using the positive integer $(i+1)r$, hence we have that $z^{(i+1)r}$ must be linear on $[\beta, z^{-(i+1)r}(\alpha)]$ and we can equate the two derivatives computed above to get $a^i b = a^{i-1} b \frac{d}{dt}z^r(t)$ on the interval $[z^{-ir}(\beta), z^{-(i+1)r}(\alpha)]$. We simplify both sides and get the thesis of the Claim. \square

By sending $i \rightarrow \infty$ in Claim 2 we see that the slope of z^r around τ^- must be equal to $a < 1$. However, since the restriction $z^r|_{[\eta, \tau]} \in \text{PL}_+^<([\eta, \tau])$, we must have that $\left. \frac{d}{dt}z^r(t) \right|_{t=\tau^-} > 1$, which is a contradiction. Therefore A is a discrete subgroup of \mathbb{R}_+ and so it is isomorphic with \mathbb{Z} . \square

Theorem 4.4.20. *Let $J = [\eta, \zeta] \subseteq [0, 1]$ be a closed interval with endpoints in S and $z \in \text{PL}_{S,G}(J)$, then:*

(1) $C_{\text{PL}_{S,G}(I)}(z)$ is isomorphic with a direct product of copies of \mathbb{Z} 's and $\text{PL}_2(J_i)$'s for some suitable intervals $J_i \subseteq I$.

(2) For every positive integer n we can decide whether or not $\sqrt[n]{z}$ exists.

Proof. The proofs of (1) and (2) follow from the proofs of Propositions 4.2.1 and 4.2.2 by replacing every occurrence of ∂_2 with ∂_S and by applying the previous corollary to get the centralizers of elements in $\text{PL}_{S,G}^0(J)$. Moreover, to prove

(2) we need to observe that, in order to start the procedure, we need to verify whether or not $\sqrt[n]{z'(\eta^+)} \in S$. \square

The following is an immediate generalization of Proposition 4.2.4:

Proposition 4.4.21 (Intersection of Centralizers). *Let $J = [\eta, \zeta] \subseteq [0, 1]$ be a closed interval with endpoints in S , let $z_1, \dots, z_k \in \text{PL}_{S,G}(J)$ and define the subgroup $C := C_{\text{PL}_{S,G}(J)}(z_1) \cap \dots \cap C_{\text{PL}_{S,G}(J)}(z_k)$. If the interval J is divided by the points in the union $\partial_S D(z_1) \cup \dots \cup \partial_S D(z_k)$ into the intervals J_i then*

$$C = C_{J_1} \cdot C_{J_2} \cdot \dots \cdot C_{J_r},$$

where $C_{J_i} := \{f \in C \mid f(t) = t, \forall t \notin J_i\} = C \cap \text{PL}_{S,G}(J_i)$. Moreover, each C_{J_i} is isomorphic to either \mathbb{Z} , or $\text{PL}_{S,G}(J_i)$ or the trivial group. \square

Corollary 4.4.22. *Let $J = [\eta, \zeta] \subseteq [0, 1]$ be a closed interval with endpoints in S and $y, z \in \text{PL}_{S,G}^0(J)$. Then $C_{\text{PL}_{S,G}(J)}(y, z)$ is either empty or countable.*

Proof. Suppose that the set $C_{\text{PL}_{S,G}(J)}(y, z)$ is not empty, then we have that $C_{\text{PL}_{S,G}(J)}(y, z) = g_0 \cdot C_{\text{PL}_{S,G}(J)}(y)$ for a suitable $g_0 \in \text{PL}_{S,G}(J)$. Thus $\#C_{\text{PL}_{S,G}(J)}(y, z) = \#C_{\text{PL}_{S,G}(J)}(y) = \aleph_0$ which is countable by Theorem 4.4.19. \square

In order to solve the conjugacy problem in $\text{PL}_{S,G}(I)$, we need to check whether or not there are candidate conjugators in a given interval of initial slopes.

Lemma 4.4.23. *Let $J = [\eta, \zeta]$ be a closed interval with endpoints in S and let $W = [w, 1] \cap G$ for some number $w \in \mathbb{R}$. If $y, z \in \text{PL}_{S,G}^0(J)$, then the set*

$$\{g'(\eta^+) \mid g \in C_{\text{PL}_{S,G}(J)}(y, z)\} \cap W$$

is contained in a finite set V that can be constructed directly.

Proof. We will use the notation of Theorem 4.4.19. Since the argument of this proof will be based on the Stair Algorithm, which works in $\text{PL}_+(J)$, we can restrict our attention on the interval between η and the first fixed point of z . Hence, we can assume $y, z \in \text{PL}_+^<(J)$ without loss of generality. We choose a positive integer r following the proof of Proposition 4.1.17: that is, we choose the smallest integer r such that

$$\min\{z^{-r}(\alpha), y^{-r}(\eta + w(\alpha - \eta))\} > \beta.$$

using the lowest possible initial number w . Using the explicit conjugator formula for an initial slope $q \in W$ (see Corollary 4.1.21), we know that the candidate conjugator has the shape $g_q := y^{-r}g_{0,q}z^r$ on the interval $[\eta, z^{-r}(\alpha)]$ for a suitable map $g_{0,q}$ that has initial slope $q \in W$. Our choice of r guarantees that, for any $q \in W$, the map g_q lies inside the final linearity box at the point $z^{-r}(\alpha)$.

Claim: Choose an integer i such that $z^{-ir}(\beta) > z^{-r}(\alpha)$. Then z^r must have a breakpoint $p \in [z^{-ir}(\beta), z^{-(i+1)r}(\alpha)]$.

Proof of the Claim. Let $a = \left. \frac{d}{dt}z^r(t) \right|_{t=\eta^+} < 1$. If z^r were linear on $[z^{-ir}(\beta), z^{-(i+1)r}(\alpha)]$ then, by Step 3 of Theorem 4.4.20, we would have that z^r is linear on every interval $[z^{-k(r)}(\beta), z^{-(i+1)r}(\alpha)]$ with slope a for every positive integer $k \geq 2$. Arguing as in the conclusion of Theorem 4.4.20, this would imply that $\left. \frac{d}{dt}z^r(t) \right|_{t=\zeta^-} = a < 1$ which is a contradiction. \square

By construction, the map $g_{0,q}$ can be built to be linear on the interval $[\eta, z^{-(i+1)r}(\alpha)]$. We observe that z^r has a breakpoint at p , hence g_0z^r must have a breakpoint at p . Now, for the map $y^{-r}g_{0,q}z^r$ to be a candidate conjugator, it must be linear around the point p , thus the breakpoints of $g_{0,q}z^r$ on the interval $[z^{-ir}(\beta), z^{-(i+1)r}(\alpha)]$ must be canceled by the set $\{c_1, \dots, c_v\}$ of all the breakpoints of y^{-r} on $[\eta, \zeta]$, thus the image of p under $g_{0,q}z^r$ must go to a breakpoint of y^{-r} . Since

$g_{0,q}z^r(p) = q(z^r(p) - \eta) + \eta \in \{c_1, \dots, c_v\}$, then there are only finitely many choices for $q \in W$. \square

Remark 4.4.24. Since the finite set V of Lemma 4.4.23 can be computed directly, we can run the stair algorithm on all elements of V as possible initial slopes and thus find all possible conjugators with slopes in $[w, 1] \cap G$.

4.5 Simultaneous Conjugacy Problem in $\text{PL}_{S,G}(I)$

In this section we wrap up all the arguments of the Chapter to solve the k -simultaneous conjugacy problem. We will first deal with the case $k = 1$ and then with the general case. Unlike the approach adopted in the first part of the paper for the case of F , in this second part we have first solved the conjugacy problem in the special case of $y = z$ before approaching the conjugacy problem for two elements $y, z \in \text{PL}_{S,G}(I)$.

4.5.1 The Ordinary Conjugacy Problem for $\text{PL}_{S,G}(I)$

Theorem 4.5.1. *The conjugacy problem in $\text{PL}_{S,G}(I)$ is solvable.*

Proof. Let $y, z \in \text{PL}_{S,G}(I)$, $y \neq z$. We use Proposition 4.4.15 and suppose that $\partial_S D(y) = \partial_S D(z) = \{0 = \alpha_0 < \alpha_1 < \dots < \alpha_r < \alpha_{r+1} = 1\}$. Now we restrict to an interval $J_i = [\alpha_i, \alpha_{i+1}]$. For simplicity, we still call $y|_{J_i}$ and $z|_{J_i}$ y and z . In order for y and z to be conjugate, we must have $y'(\alpha_i^+) = z'(\alpha_i^+)$ and $y'(\alpha_{i+1}^-) = z'(\alpha_{i+1}^-)$. Up to taking inverses of y and z , we can assume that $q = y'(\alpha_i^+) = z'(\alpha_i^+) < 1$. Now observe that $g^{-1}yg = z$ if and only if $(y^v g)^{-1}y(y^v g) = z$ for every $v \in \mathbb{Z}$. If $q^{\rho(g)}$

is the initial slope of g , then $q^{v+\rho(g)}$ is the initial slope of $y^v g$. Thus, up to taking powers of y we can assume that the exponent of the initial slope of g is in $[q, 1]$. By Lemma 4.4.23, the set of possible initial slopes inside $[q, 1] \cap G$ is finite and can be directly constructed, so we can apply the Stair Algorithm on each of them and verify if any of the obtained maps is a conjugator. All the other conjugators are found by taking the products $y^v g$ with $v \in \mathbb{Z}$. \square

4.5.2 The k -Simultaneous Conjugacy Problem in $\text{PL}_{S,G}(I)$

The algorithm used to solve the k -simultaneous problem in the case of the group F can be extended in full generality, except for one of its steps.

Theorem 4.5.2. *The k -simultaneous conjugacy problem in $\text{PL}_{S,G}(I)$ is solvable .*

Proof. To prove the solvability of the k -simultaneous conjugacy problem we can mimic completely the proof used for Thompson's group F . We need to replace every occurrence of ∂_2 with ∂_S and speak of elements of S instead of dyadic rational numbers. The only part in which we need refine the argument is in the case of Subsection 4.3.2 in which we reduce to solve the equation

$$x^m = g_0 \widehat{y}^n \tag{4.4}$$

where $x, y, g_0 \in \text{PL}_{S,G}([\eta, \zeta])$ are given and we are looking for $m, n \in \mathbb{Z}$ satisfying the previous equation. We define $q = g'_0(\eta^+) \in \mathbb{R}_+$ and so $x'(\eta^+) = q^\alpha, y'(\eta^+) = q^\beta, g'_0(\eta^+) = q$ for some $\alpha, \beta \in \mathbb{R}$. Notice that in Subsection 4.3.2 we have $\alpha, \beta, \gamma \in \mathbb{Z}$, while here not all of them are integers. We must then have

$$q^\alpha = x'(\eta^+)^m = (g_0 \widehat{y}^n)'(\eta^+) = q^{1+\beta n} \tag{4.5}$$

and therefore we need to solve the equation

$$\alpha m = 1 + \beta n \tag{4.6}$$

for some $m, n \in \mathbb{Z}$. We observe that if equation (4.6) is solvable, then α is rational if and only if β is rational. Thus, if either α or β is a rational number it is immediate to check whether there is a solution to (4.6). If α and β are both irrational, then equation (4.6) becomes a \mathbb{Q} -linearity dependence relation and, if it is solvable, then the dimension of the vector space generated by α, β and 1 over \mathbb{Q} is exactly 2. By Remark 4.4.8 and the last of the requirements in Remark 4.4.7 we are able to detect if this last statement is true or not. In case it is true, then there is a unique solution to (4.6) and it is given by the coordinates of 1 in the basis α and β , thus it is now trivial to check if there is a integer solution or not. In case there is a solution to equation (4.6), we do not need to find a bound for $m, n \in \mathbb{Z}$ as for the case of Thompson's group F , because there is at most one solution. The remaining part of the algorithm follows as before. \square

4.6 Interesting Examples

Now that we have developed the general theory, we are going to see a few interesting examples where the simultaneous conjugacy problem is solvable. We will not dwell too much on the details here, sketching only why it is possible to verify the requirements.

Example 4.6.1. $S = \mathbb{Q}$ and $G = \mathbb{Q}^* = \mathbb{Q} \cap (0, \infty)$.

Since \mathbb{Q} is a field, $S/I = \{0\}$ so all the requirements of Remark 4.4.7 are satisfied. To solve the simultaneous conjugacy problem, we need to solve equation (4.5),

which becomes

$$\frac{a_1^m}{b_1^m} = \frac{ca_2^n}{db_2^n}$$

where we can assume that all numerators are coprime with the denominators. By equating prime factors in the equation to be solved, we get a system of equations of the type $\alpha_i m = \gamma_i + \beta_i n$, for $\alpha_i, \beta_i, \gamma_i \in \mathbb{Z}$. All of them can be solved in the same fashion as in Lemma 4.3.4 and we can reduce equation (4.4) to the equation $X^k = G_0 Y^k$ and solve it as in Subsection 4.3.2.

Example 4.6.2. $S = \mathbb{Z}[\frac{1}{n_1}, \dots, \frac{1}{n_k}]$ and $G = \langle n_1, \dots, n_k \rangle$ for $n_1, \dots, n_k \in \mathbb{Z}$.

We observe that $S = \mathbb{Z}[\frac{1}{n_1 \dots n_k}]$ and it can be shown that, if $r := n_1 \dots n_k$, then $S/I \cong \mathbb{Z}/r\mathbb{Z}$ as rings and therefore the requirements of Remark 4.4.7 are also satisfied. Equation (4.5) can be treated as in the previous example. For $k = 1$, we recall that the groups $\text{PL}_{S,G}(I)$ are known as *generalized Thompson's groups*.

Example 4.6.3. $S = \mathbb{Z}[\frac{1}{n_1}, \dots, \frac{1}{n_k}, \dots]$ with $G = \langle \{n_i\}_{i \in \mathbb{N}} \rangle$ for a sequence $\{n_i\}_{i \in \mathbb{N}} \subseteq \mathbb{Z}$.

This example is easily reducible to the previous one, since if we are given a finite set E of elements in $\text{PL}_{S,G}(I)$ we can consider the set $\{n_{i_1}^{\alpha_{i_1}}, \dots, n_{i_v}^{\alpha_{i_v}}\}$ of all slopes of elements of E . Then $E \subseteq \text{PL}_{S',G'}(I)$ where $S' := \mathbb{Z}[\frac{1}{n_{i_1}}, \dots, \frac{1}{n_{i_v}}]$ and $G' := \langle n_{i_1}, \dots, n_{i_v} \rangle$.

Example 4.6.4. S finite algebraic extension over \mathbb{Q} and $G = S^* := S \cap (0, \infty)$

As with the first example, since S is a finite algebraic extension it is not difficult to verify that all the requirements of Remark 4.4.7 are satisfied.

Example 4.6.5. $S = \mathbb{R}$ and $G = \mathbb{R}_+$

In order to verify the requirements for this case, we need to discuss exactly what we mean by real number and how we implement it in a machine. In most cases, we work with numbers which are expressed as roots of polynomials in some subfields of \mathbb{R} and we are able to give a complete answer and the same is true for all the requirements of Remark 4.4.7.

CHAPTER 5

CRYPTANALYSIS OF THE SHPILRAIN-USHAKOV PROTOCOL FOR
THOMPSON'S GROUP

5.1 Introduction

Public Key Cryptography is involved in the exchange of information between two parties A and B , often labeled as “Alice” and “Bob”. Before they start sending data to the other party, they must agree on a way to send it. The type of encryption they use is called “public key” because part of information they need to agree on (in this context it is usually a group and some of its subgroups or elements) and the encryption scheme are in the public domain. Alice and Bob each choose secretly some information, respectively i_A and i_B . They both use their secret information to encrypt some public data w , and send it to the other party. Alice receives the encrypted information $e(i_B, w)$ and she encrypts it using her own information, obtaining some data $e(i_A, e(i_B, w))$. Similarly, Bob receives $e(i_A, w)$ and encrypts it using i_B to get $e(i_B, e(i_A, w))$. The public protocol is usually chosen so that after this procedure they obtain the same information, that is $e(i_A, e(i_B, w)) = e(i_B, e(i_A, w))$. This common information is now referred to as the *shared secret key* and it is now used to exchange messages between the two parties. This “commutativity” of encryption comes from generalizing the Diffie-Hellman cryptosystem based on the infinite cyclic group (see [33] for details).

A third party E (“Eve”) is listening and detecting anything the two parties are exchanging. Thus Eve captures $e(i_A, w)$ and $e(i_B, w)$ and any message encrypted using the shared secret key. To break the protocol Eve must try to extract i_A and i_B or equivalent elements. This discussion will be made precise

in the next sections, by describing precisely the Shpilrain-Ushakov public key cryptography protocol based on Thompson's group F and how the information gets transmitted between the two parties.

The Chapter is organized as follows. In Section 5.2 and Section 5.3 we recall the protocol. In Section 4 we recall the choice of parameters proposed in [61]. In section 5.5 we give an efficient attack that always recovers the secret key. In Sections 5.6 and 5.7 we show another type of attack. In Section 5.8 we make some comments on possible generalizations of this protocol. The material of this Chapter is going to appear in the *Journal of Cryptology* [49].

History and related works.

The first attack on this protocol was announced by Ruinskiy, Shamir and Tsaban in November 2005 at the Bochum Workshop *Algebraic Methods in Cryptography*, showing that the parameters given in [61] should be increased to have higher security of the system. Their attack was improved in other announcements and was finalized in [56] at the same time that the material of this Chapter was written. Their attack describes a more general procedure which uses length functions. We remark that the same authors have been developing new techniques involving "subgroup distance functions" and that they applied them to the same protocol for F as a test case [57]. The approach of Ruinskiy, Shamir and Tsaban in their papers is heuristic, and its success rates are good but not 100%. Our approach is deterministic, and provably succeeds in all possible cases.

5.2 The Protocol

The protocol proposed in [61] is based on the *decomposition problem*: given a group G , a subset $X \subseteq G$ and $w_1, w_2 \in G$, find $a, b \in X$ with $aw_1b = w_2$, given that such a, b exist. Here is the protocol in detail:

Public Data.

A finitely presented group G , an element $w \in G$ and two subgroups A, B of G such that $ab = ba$ for all $a \in A, b \in B$.

Private Keys and Communication.

Alice chooses $a_1 \in A, b_1 \in B$ and sends the element $u_1 = a_1wb_1$ to Bob. Bob chooses $b_2 \in B, a_2 \in A$ and sends the element $u_2 = b_2wa_2$ to Alice. Alice then computes the element $K_A = a_1u_2b_1 = a_1b_2wa_2b_1$ and Bob computes the element $K_B = b_2u_1a_2 = b_2a_1wb_1a_2$. Since A and B commute elementwise, $K = K_A = K_B$ becomes Alice and Bob's shared secret key to send one bit. Alice and Bob need to generate and compute a shared secret key for each bit they want to send.

To communicate bits, the two parties send elements $x \in G$. If Alice wants to send a 1, she uses the relations of G to rewrite the word representing K , "scrambling" the way it appears, and sends it. If she wants to send a 0, she chooses a random element $x \in G$ and sends it; with overwhelming probability she will pick an element different from K . Now Bob solves the word problem for xK^{-1} , to identify whether he has received a 0 or a 1. Hence, it is important for the

word problem to be efficient in the group.

Eavesdropper's Data and Brute force Attack.

Eve has all the public data and the two elements u_1 and u_2 , observed during Alice and Bob's exchange.

To break the protocol To recover a_1 , Eve needs to find a pair (\bar{a}, \bar{b}) such that

$$u_1 = \bar{a}w\bar{b}$$

Thus Eve computes

$$\bar{a}u_2\bar{b} = \bar{a}b_2wa_2\bar{b} = b_2\bar{a}w\bar{b}a_2 = b_2u_1a_2 = K.$$

Eve can always use what is called a *brute force attack*, that is, try all the elements of A to get candidates for the shared secret key to test on the exchanged message. However, as the groups A and B are usually chosen to be infinite, this is a cumbersome and slow way to look for a suitable pair (\bar{a}, \bar{b}) and she has to look for something more efficient.

5.3 The Subgroups A_s, B_s

Now we apply the protocol described in the previous Section to the special case of $G = F$ Thompson's group with the standard generating set defined in Chapter 1. We introduce a notation which will be useful for the definition of the subgroups A and B . For every positive integer k we call

$$\varphi_k := 1 - \frac{1}{2^{k+1}}.$$

From the definition of x_k , we get

$$x_k^{-1}([\varphi_k, 1]) = [\varphi_{k+1}, 1] \subseteq \left[\frac{3}{4}, 1\right]$$

implying that, for $t \in [\varphi_k, 1]$, we have

$$\frac{d}{dt}x_0x_k^{-1}(t) = x'_0(x_k^{-1}(t))(x_k^{-1})'(t) = 2 \cdot \frac{1}{2} = 1$$

which means $x_0x_k^{-1}$ is the identity in the interval $[\varphi_k, 1]$. For any $s \in \mathbb{N}$, Shpilrain and Ushakov define in [61] the following sets

$$S_{A_s} = \{x_0x_1^{-1}, \dots, x_0x_s^{-1}\}$$

and

$$S_{B_s} = \{x_{s+1}, \dots, x_{2s}\}$$

and then define the subgroups $A_s := \langle S_{A_s} \rangle$ and $B_s := \langle S_{B_s} \rangle$. The previous argument immediately yields that all elements of A_s commute with all elements of B_s (see figure 5.1), i.e.

Lemma 5.3.1 (Shpilrain-Ushakov [61]). *For every fixed $s \in \mathbb{N}$, $ab = ba$ for every elements $a \in A_s$ and $b \in B_s$.*

Convention 5.3.2. For this Chapter only, for every dyadic number $d \in [0, 1]$ we denote by $\text{PL}_2([0, d])$ the set of functions in $\text{PL}_2(I)$ which are the identity on $[d, 1]$. Moreover, if we are given a piecewise linear map defined only on $[0, d]$ we will assume it is extended to $[0, 1]$ by defining it as the identity on $[d, 1]$. Similar remarks apply to $\text{PL}_2([d, 1])$.

Parts (i) and (iii) of the following Lemma are in [61], while part (ii) is a simple observation.

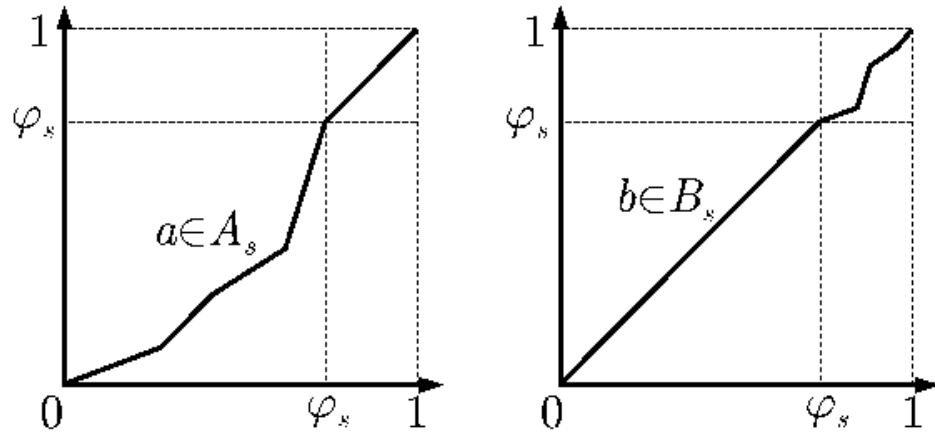


Figure 5.1: An example of an element of A_s and one of B_s .

Lemma 5.3.3. (i) A_s is the set of elements whose normal form is of the type

$$x_{i_1} \dots x_{i_m} x_{j_m}^{-1} \dots x_{j_1}^{-1}$$

where $i_k - k < s$ and $j_k - k < s$, for all $k = 1, \dots, m$.

(ii) $B_s = \text{PL}_2([\varphi_s, 1])$.

(iii) Let $a \in A_s$ and $b \in B_s$ be such that their normal forms are

$$a = x_{i_1} \dots x_{i_m} x_{j_m}^{-1} \dots x_{j_1}^{-1}$$

$$b = x_{c_1} \dots x_{c_u} x_{d_v}^{-1} \dots x_{d_1}^{-1}.$$

Then the normal form of ab is

$$ab = x_{i_1} \dots x_{i_m} x_{c_1+m} \dots x_{c_u+m} x_{d_v+m}^{-1} \dots x_{d_1+m}^{-1} x_{j_m}^{-1} \dots x_{j_1}^{-1}.$$

Theorem 5.3.4 (Shpilrain-Ushakov [61]). In Thompson's group F , the normal form of a given word w can be computed in time $O(|w| \log |w|)$, where $|w|$ is the length of the normal form in the generators x_0, x_1, x_2, \dots .

5.4 Suggested Parameters for the Encryption

We now illustrate briefly the choice of parameters proposed in [61]. Alice and Bob select an integer $s \in [3, 8]$ and an even integer $M \in [256, 320]$ uniformly and randomly. Moreover, they also choose a random element $w \in \langle x_0, x_1, \dots, x_{s+2} \rangle$ with $|w| = M$, where $|w|$ is as in Theorem 5.3.4. The numbers s, M and the element w are now part of the public data.

To proceed with the protocol described in Section 5.2, Alice chooses random elements $a_1 \in A_s, b_1 \in B_s$, with $|a_1| = |b_1| = M$, while Bob chooses random elements $a_2 \in A_s, b_2 \in B_s$, with $|a_2| = |b_2| = M$. Now they both compute the shared secret key:

$$K = a_1 b_2 w a_2 b_1.$$

Shpilrain and Ushakov remark that this choice of parameters gives a key space which increases exponentially in M , i.e., $|A_s(M)| \geq \sqrt{2}^M$, thereby making it difficult for Eve to perform a brute force attack.

5.5 Recovering the Shared Secret Key

We begin this section by providing the theoretical background for the attack. We will use the piecewise-linear point of view to understand why the attack works and then rephrase it combinatorially. We will now describe how Eve, by knowing the elements w, u_1, u_2 , can always recover one of the two legitimate parties' private keys. She chooses whose key to crack, depending on whether the graph of w is above or below the point (φ_s, φ_s) .

5.5.1 Recovering Bob's Private Keys: $w(\varphi_s) \leq \varphi_s$

Since $w(t) \leq \varphi_s$ for all $t \in [0, \varphi_s]$, we observe the following identity

$$u_2(t) = b_2 w a_2(t) = w a_2(t), \quad \forall t \in [0, \varphi_s].$$

Therefore, Eve may apply w^{-1} to the left of both sides of the previous equation to obtain

$$w^{-1} u_2(t) = a_2(t), \quad \forall t \in [0, \varphi_s]$$

and so $w^{-1} u_2 \in A_s B_s$ and

$$a_2(t) = \begin{cases} w^{-1} u_2(t) & t \in [0, \varphi_s] \\ t & t \in [\varphi_s, 1]. \end{cases}$$

Now Eve has the elements a_2 , w and $u_2 = b_2 w a_2$ and she computes

$$b_2 = u_2 a_2^{-1} w^{-1}$$

thereby detecting Bob's private keys and the shared secret key K .

5.5.2 Recovering Alice's Private Key: $w(\varphi_s) > \varphi_s$

Since $w^{-1}(t) < \varphi_s$ for all $t \in [0, \varphi_s]$, we have

$$u_1^{-1}(t) = b_1^{-1} w^{-1} a_1^{-1}(t) = w^{-1} a_1^{-1}(t), \quad \forall t \in [0, \varphi_s].$$

By applying the same technique as in the previous subsection Eve recovers a_1^{-1} and obtains that $u_1 w^{-1} \in A_s B_s$. Thus, she is able to detect a_1, b_1 and the shared secret key K . Alternatively, Eve observes

$$w^{-1} u_1(t) = w^{-1} a_1 w b_1(t) = b_1(t), \quad \forall t \in [\varphi_s, 1]$$

and so

$$b_1(t) = \begin{cases} t & t \in [0, \varphi_s] \\ w^{-1}u_1(t) & t \in [\varphi_s, 1]. \end{cases}$$

5.5.3 Outline of the attack

We expand on the previous discussion to describe a combinatorial attack. Assume that Eve has the elements w, u_1, u_2 .

1. Eve writes the normal forms of $z_1 := u_1 w^{-1}$ and $z_2 := w^{-1} u_2$.
2. By the previous discussion, either $z_1 \in A_s B_s$ or $z_2 \in A_s B_s$ (or both). She can detect which one using Lemma 5.3.3(i) and selects this z_i .
3. She computes the A_s -part a_{z_i} of z_i .
4. If $i = 1$, she computes $b_{z_1} := w^{-1} a_{z_1}^{-1} u_1$. If $i = 2$, she computes $b_{z_2} := u_2 a_{z_2}^{-1} w^{-1}$.
5. Eve computes K from $u_1, u_2, a_{z_i}, b_{z_i}$.

The only point of this procedure which needs further explanation is (2). When we have the normal forms of z_1, z_2 , we know that one of them is in $A_s B_s$. We write the normal form $z_i = x_{i_1} \dots x_{i_e} x_{j_f}^{-1} \dots x_{j_1}^{-1}$ and we look at the notation of Lemma 5.3.3(i): we need to find the smallest index r in z_i such that either i_{r+1} or j_{r+1} does not satisfy the index condition in Lemma 5.3.3(i). To verify if $z_i \in A_s B_s$, we need to check whether it has the form described in Lemma 5.3.3(iii): we remove the first r letters and the last r letters of z_i from the word and we lower all the indices of the remaining letters by r ; if what remains is a word whose indices are in $\{s+2, \dots, 2s\}$, then we have an element of B_s , otherwise $z_i \notin A_s B_s$. If $z_i \in A_s B_s$, then a_{z_i} will be the product of the first r elements of z_i and the last r ones.

5.5.4 Complexity of the attack.

By Theorem 5.3.4 we know that computing normal forms can be done in time $O(M \log M)$, where M is the size of the inputs suggested in Section 5.4. Part (2) of the attack can be executed in time $O(M)$, by just reading the indices of the normal forms and finding when the relation of Lemma 5.3.3(i) breaks down. Finally, the last steps are just multiplications and then simplifications so they can again be performed in time $O(M \log M)$. Therefore, Eve can recover the shared secret key in time $O(M \log M)$.

Remark 5.5.1. The previous discussion shows that there is no need to pass from words to piecewise-linear functions and back. The attack can be performed entirely by using the combinatorial point of view which is used for encryption. The piecewise-linear point of view is necessary only to prove that the combinatorial attack works. We also remark that the complexity of the attack is independent of the parameter s .

5.6 Transitivity of A_s and B_s

The previous section showed how to recover the shared secret key of one of the two involved parties, based on whether the graph of w lies above or below the point (φ_s, φ_s) . However, it is possible to find the shared secret key even in the cases not studied in the previous section. More precisely, it is possible to attack Alice's word in the case $w(\varphi_s) \leq \varphi_s$ and Bob's word in the case $w(\varphi_s) > \varphi_s$. We need a better description of the subgroups A_s . If $s = 1$, we observe that $A_1 = \langle x_0 x_1^{-1} \rangle$ is a cyclic group. For larger values of s , A_s becomes the full group of piecewise linear homeomorphism on $[0, \varphi_s]$.

Theorem 5.6.1. $A_s = \text{PL}_2([0, \varphi_s])$, for every $s \geq 2$.

In order to prove the Theorem we need the following two Lemmas.

Lemma 5.6.2. $x_0^{-1}\text{PL}_2([0, \varphi_s])x_0 = \text{PL}_2([0, \varphi_{s+1}])$. Similarly, $x_0^{-1}\text{PL}_2([\varphi_s, 1])x_0 = \text{PL}_2([\varphi_{s+1}, 1])$.

Proof. This result is a special case of Theorem 1.1.5, but it is straightforward to verify it too. Observe that $x_0^{-1}(\varphi_s)$ is fixed by $x_0^{-1}fx_0$ for every $f \in \text{PL}_2([0, \varphi_s])$ and

$$x_0^{-1}(\varphi_s) = \frac{1}{2} \left(1 - \frac{1}{2^{s+1}} - \frac{1}{2} \right) + \frac{3}{4} = \varphi_{s+1}$$

therefore the result holds. The other result follows similarly. \square

The next corollary is also a special case of Theorem 1.1.5.

Corollary 5.6.3. $\text{PL}_2([0, \varphi_s]) \cong \text{PL}_2([\varphi_s, 1]) \cong F$, for every $s \geq 0$.

Lemma 5.6.4. $A_2 = \text{PL}_2\left(\left[0, \frac{7}{8}\right]\right)$.

Proof. Define $a = (\rho_2^*)^{-1}(x_0)$ and $b = (\rho_2^*)^{-1}(x_1)$ (see figure 5.2). Then

$$a(t) = \begin{cases} \frac{1}{2}t & t \in \left[0, \frac{1}{4}\right] \\ \left(t - \frac{1}{4}\right) + \frac{1}{8} & t \in \left[\frac{1}{4}, \frac{3}{8}\right] \\ 2\left(t - \frac{3}{8}\right) + \frac{1}{4} & t \in \left[\frac{3}{8}, \frac{1}{2}\right] \\ t & t \in \left[\frac{1}{2}, 1\right] \end{cases} \quad b(t) = \begin{cases} t & t \in \left[0, \frac{1}{4}\right] \\ \frac{1}{2}\left(t - \frac{1}{4}\right) + \frac{1}{4} & t \in \left[\frac{1}{4}, \frac{3}{8}\right] \\ \left(t - \frac{3}{8}\right) + \frac{5}{16} & t \in \left[\frac{3}{8}, \frac{7}{16}\right] \\ 2\left(t - \frac{7}{16}\right) + \frac{3}{8} & t \in \left[\frac{7}{16}, \frac{1}{2}\right] \\ t & t \in \left[\frac{1}{2}, 1\right] \end{cases}$$

One sees that $a = x_0^2 x_1^{-1} x_0^{-1}$ and that $b = x_0 x_1^2 x_2^{-1} x_1^{-1} x_0^{-1}$ (for example this can be verified using tree diagrams for F , i.e. using Proposition 1.3.3 in [5] or by a

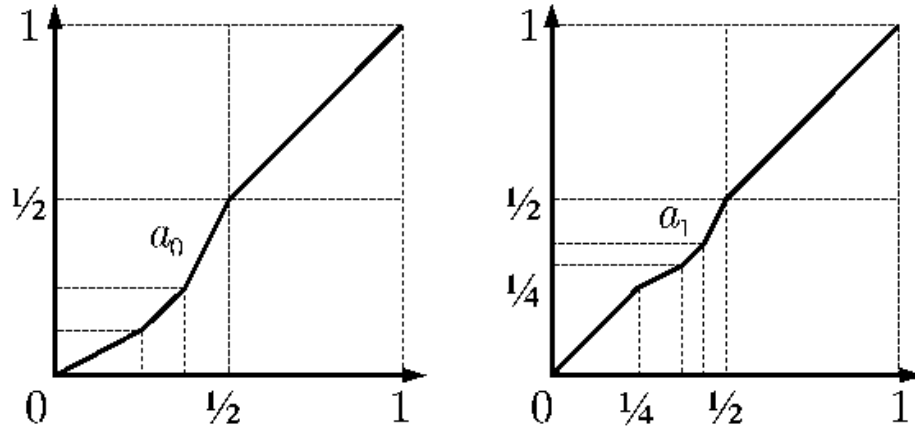


Figure 5.2: The two standard generators for $\text{PL}_2([0, \varphi_2])$.

direct computation). Since ρ_2^* is an isomorphism, $\text{PL}_2([0, \frac{1}{2}]) = \langle a, b \rangle$ and, by Lemma 5.6.2, $\text{PL}_2([0, \frac{7}{8}]) = \langle x_0^2 a x_0^{-2}, x_0^2 b x_0^{-2} \rangle$. By Lemma 5.3.3 we have

$$x_0^2 a x_0^{-2} = x_0^4 x_1^{-1} x_0^{-3} \in A_2$$

$$x_0^2 b x_0^{-2} = x_0^3 x_1^2 x_2^{-1} x_1^{-1} x_0^{-3} \in A_2$$

so that $\text{PL}_2([0, \frac{7}{8}]) \subseteq A_2$. The other inclusion is obvious. \square

Proof of Theorem 5.6.1. By Lemma 5.6.4 we have that $A_2 = \text{PL}_2([0, \varphi_2])$ and so, by applying Lemma 5.6.2 and the definition of A_s we have

$$\text{PL}_2([0, \varphi_s]) = x_0^{s-2} A_2 x_0^{2-s} \subseteq A_s \subseteq \text{PL}_2([0, \varphi_s])$$

therefore implying that $A_s = \text{PL}_2([0, \varphi_s])$. \square

Corollary 5.6.5. $A_s \cong B_s \cong F$, for every $s \geq 2$.

The previous Theorem and Lemma 4.1.5 in Chapter 4 yield the following corollaries:

Corollary 5.6.6 (Transitivity of A_s). *For any $t_1, t_2 \in \mathbb{Z} \left[\frac{1}{2} \right] \cap [0, \varphi_s]$ we can construct an $a \in A_s$ with $a(t_1) = t_2$.*

Proof. We appeal to the transitivity of F on the dyadic numbers of $[0, 1]$. We use the map ρ_s of Lemma 5.6.3 and pull back a_1, a_2 to $[0, 1]$ as $\rho_s^{-1}(a_1), \rho_s^{-1}(a_2)$. We consider the two dyadic partitions $0 < \rho_s^{-1}(a_1) < 1$ and $0 < \rho_s^{-1}(a_2) < 1$ of the interval $[0, 1]$ and apply Lemma 1.1.4 to find $f \in F$ with $f(\rho_s^{-1}(a_1)) = \rho_s^{-1}(a_2)$. Then the element $(\rho_s^*)^{-1}(f) \in A_s$ satisfies the requirements. \square

Corollary 5.6.7 (Extendability of A_s). *Let $t_0 \in \mathbb{Z} \left[\frac{1}{2} \right] \cap [0, \varphi_s]$ and $\bar{a}(t) = a|_{[0, t_0]}$ for an element $a \in A_s$. Assume we know \bar{a} , but that we do not know a . Then we can construct an $a_\sigma \in A_s$ such that $a_\sigma(t) = \bar{a}(t)$ for all $t \in [0, \varphi_s]$.*

Proof. We observe that $\rho_s^*(\bar{a})$ is a piecewise linear map between two intervals with dyadic extremes and contained in $[0, 1]$. We apply Lemma 4.1.5 to extend $\rho_s^*(\bar{a})$ to a piecewise linear homeomorphism $f \in F$. Then we pull back f to A_s through $(\rho_s^*)^{-1}(f)$ which satisfies the requirements. \square

Remark 5.6.8. The analogues of the last two corollaries are true for the interval $[\varphi_s, 1]$ and B_s too.

5.7 Using Transitivity to Attack the Shared Secret Key

With the new description of A_s and B_s given in section 5.6, it is now possible to attack the secret keys in the cases left open from section 5.5.

5.7.1 Attacking Alice's word for the case $w(\varphi_s) \leq \varphi_s$

We have

$$u_1(t) = a_1 w(t), \forall t \in [0, \varphi_s],$$

thus

$$a_1(t) = u_1 w^{-1}(t), \forall t \in [0, w(\varphi_s)]$$

and so a_1 is uniquely determined in $[0, w(\varphi_s)]$. We apply corollary 5.6.7 to find an element $a_\sigma \in A_s$ such that $a_\sigma = a_1$ on the interval $[0, w(\varphi_s)]$. If we define

$$b_\sigma := w^{-1} a_\sigma^{-1} u_1$$

then we have that

$$b_\sigma(t) = w^{-1} a_\sigma^{-1} a_1 w(t) = w^{-1} w(t) = t, \forall t \in [0, \varphi_s]$$

Therefore $b_\sigma \in B_s$ and $a_\sigma w b_\sigma = u_1$ and so Eve can recover the shared secret key K by using the pair (a_σ, b_σ) .

Remark 5.7.1. We observe that any extension of $a_1|_{[0, w(\varphi_s)]}$ to an element a_σ of $\text{PL}_2([0, \varphi_s])$ will yield a suitable element to attack Alice's key. Moreover, any element $a'_1 \in A_s$ such that $a'_1 w b'_1 = u_1$, for some suitable $b'_1 \in B_s$, will be an extension of $a_1|_{[0, w(\varphi_s)]}$.

5.7.2 Attacking Bob's word for the case $w(\varphi_s) > \varphi_s$

Eve considers $u_2^{-1} = a_2^{-1} w^{-1} b_2^{-1}$ and recovers a pair $(a_\sigma^{-1}, b_\sigma^{-1})$ to get the shared secret key in the same fashion of the previous subsection.

Remark 5.7.2. Both the techniques of this section have been carried out using the transitivity of A_s (Corollary 5.6.6). They can also be solved by using the analogue of Corollary 5.6.7 for B_s to get another pair (a_σ, b_σ) which can be used to retrieve the secret key.

5.8 Comments and Alternatives to the Protocol

This section analyzes possible alternatives and weaknesses of our methods. We observe that, if instead of $\text{PL}_2(I)$ we had used a larger group of piecewise linear homeomorphisms of the unit interval, the same technique would have worked, as long as the commuting subgroups A and B had disjoint supports. More generally, we can copy this idea if the given group G acts on some space and we have A, B with disjoint support. We will now see some examples of how this is possible.

5.8.1 Choice of the subgroups A and B

We recall the following result from Chapter 4 (see Theorems 4.2.2 and 4.2.4):

Theorem 5.8.1. *Let $A = \langle a_1, \dots, a_m \rangle \leq F$ be a finitely generated subgroup. Then*

(i) *There exists a dyadic partition of $[0, 1] = I_1 \cup \dots \cup I_n$ such that the centralizer $C_F(A) := \{f \in F \mid af = fa, \forall a \in A\}$ is a product of subgroups C_1, \dots, C_n , where $C_r \leq \{f \in F \mid f(t) = t, \forall t \notin I_r\}$. Moreover, we have*

- $C_r = \text{PL}_2(I_r)$ if and only if $a_i|_{I_r} = \text{id}$, for all $i = 1, \dots, m$.

- $C_r \cong \mathbb{Z}$ if and only if $a_1|_{I_r}, \dots, a_m|_{I_r}$ have a common root on I_r .
- $C_r = 1$ if and only if there are $i \neq j$ such that $a_i|_{I_r}, a_j|_{I_r}$ have no common root on I_r .

(ii) There exist two elements $g_1, g_2 \in F$ such that $C_F(A) = C_F(g_1) \cap C_F(g_2)$.

Going back to the protocol introduced in Section 5.2 we observe that, after we choose a finitely generated subgroup $A = \langle f_1, \dots, f_m \rangle$, we are very restricted in our choice of the subgroup B . Since $B \leq C_F(A)$, we must make sure that the elements of B , when restricted to I_r , are powers of common roots of the a_i 's, if at least one a_i is non-trivial on I_r . This gives a tight restriction on the subgroup B whose support is essentially disjoint from that of A , except in the intervals where they all are powers of a common root. An attack similar to that of Section 5.5 can thus be applied on each interval I_r : if their supports are disjoint on I_r , we can act as before, otherwise elements of A and B are powers of a common root on I_r .

With more general commuting subgroups, the attack of Section 5.5 does not immediately give either of the two keys. However it is likely that a modification of the given algorithm can recover the shared secret key for any choice of commuting subgroups A and B .

5.8.2 Alternative Protocol and Attacks

Ko-Lee et al. [44] introduced a slightly different protocol based on the decomposition problem (They worked with braid groups, but we will apply their protocol to Thompson's group). In their protocol, Alice picks $a_1, a_2 \in A$ and sends

$u_1 = a_1 w a_2$ to Bob, while Bob chooses $b_1, b_2 \in B$ and sends $u_2 = b_1 w b_2$ to Alice. We can still attempt to solve this new protocol, by again dividing the problem into various cases. We assume that we use the same subgroups A_s and B_s and we work in the case $w(\varphi_s) \leq \varphi_s$ to show how to attack the private keys of Bob. We apply the analogue for B_s of Corollary 5.6.6 and find a b_0 such that $b_0^{-1}(w^{-1}(\varphi_s)) = u_2^{-1}(\varphi_s) = b_2^{-1}w^{-1}(\varphi_s)$. We define

$$\begin{aligned} b'_1 &= b_1 \\ b'_2 &= b_2 b_0^{-1} \\ u'_2 &= b'_1 w b'_2 \end{aligned}$$

so that $b'_2(w^{-1}(\varphi_s)) = w^{-1}(\varphi_s) > \varphi_s$. Thus we have

$$u'_2(t) = b'_1(t) w b'_2(t) = w b'_2(t), \forall t \in [0, w^{-1}(\varphi_s)]$$

hence

$$b'_2(t) = w^{-1}u'_2(t), \forall t \in [0, w^{-1}(\varphi_s)].$$

Thus b'_2 is uniquely determined in $[0, w^{-1}(\varphi_s)]$. We apply corollary 5.6.7 for B_s to find a $b_{\sigma_2} \in B_s$ such that $b_{\sigma_2} = b'_2$ on $[0, w^{-1}(\varphi_s)]$ and we define

$$b_{\sigma_1} := u'_2 b_{\sigma_2}^{-1} w^{-1}.$$

Thus

$$b_{\sigma_1}(t) = b'_1 w b_{\sigma_2}^{-1} w^{-1}(t) = b'_1(t) = t, \forall t \in [0, \varphi_s]$$

therefore $b_{\sigma_1} \in B_s$. Therefore the pair $(b_{\sigma_1}, b_{\sigma_2})$ satisfies $u'_2 = b_{\sigma_1} w b_{\sigma_2}$ and so Eve can recover the shared secret key K . A similar argument can be used to attack the element $a_1 w a_2$, with the transitivity results for A_s .

5.8.3 A comment on the Alternative Protocol

The weakness in the protocol discussed in the previous subsection arises from the fact that the chosen subgroups A_s and B_s are transitive on the intervals on which they act nontrivially. This suggests that a possible way to avoid such attacks is for A and B to be chosen to be not transitive on their support.

Remark 5.8.2. We observe that the attacks of section 5.7 and section 5.8 can be carried out in a fashion similar to that of Section 5.5, still producing a solution in polynomial time.

CHAPTER 6

STRUCTURE THEOREMS FOR SUBGROUPS OF HOMEOMORPHISMS GROUPS

Let $\text{Homeo}_+(S^1)$ denote the full group of orientation-preserving homeomorphisms of the unit interval and G be one of its subgroups. In this Chapter we recall the notion of *rotation number* for an element of $\text{Homeo}_+(S^1)$. This number is invariant under conjugacy and describes the behavior of an element under infinitely many iterations. Loosely speaking, it describes how close to a rotation an element is, when we iterate it many times on a point of the circle. It is a well known result that the rotation number map $\text{rot} : G \rightarrow \mathbb{R}/\mathbb{Z}$ is a group homomorphism if the group G is abelian. We give a direct proof that the same result is true if we assume that the group G has no non-abelian free subgroups. This was first deduced as a Corollary of a Theorem by Margulis in [47]. Our methods are independent and we recover Margulis's Theorem as a byproduct. We use our understanding of the rotation number map to obtain a classification of subgroups of $\text{Homeo}_+(S^1)$ and show how to build examples of such subgroups.

The Chapter is organized as follows: Section 6.1 recalls the necessary language and tools which will be used in the Chapter; Section 6.2 shows that the rotation map is a homomorphism on subgroups as above; Section 6.4 explains the main structure theorem and shows how to construct directly embeddings in $\text{Homeo}_+(S^1)$ realizing the subgroups of the structure theorem; Section 6.5 presents an analogue of Sacksteder's Theorem (see [29]) for fixed-point free subgroups, showing that they must always be abelian; Section 6.3 uses the fact that the rotation map is a homomorphism to prove Margulis' Theorem on invariant measures on the unit circle. The material of this Chapter represents joint work

with Collin Bleak and Martin Kassabov.

6.1 Background and Tools

In this section we collect some known results we will use throughout the Chapter. We begin by recalling the definition of rotation number. Given $f \in \text{Homeo}_+(S^1)$, let $F : \mathbb{R} \rightarrow \mathbb{R}$ represent one lift of f (see figure 6.1) via the standard covering projection $\exp : \mathbb{R} \rightarrow S^1$, where we think of S^1 as a subset of the complex plane and use $\exp(t) = e^{2\pi it}$.

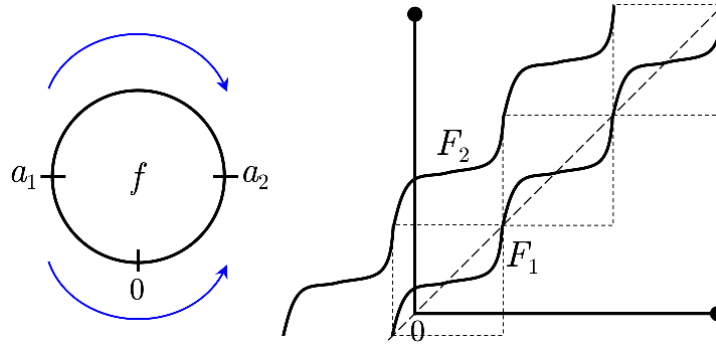


Figure 6.1: Two lifts of a circle homeomorphism.

We consider the limit

$$\lim_{n \rightarrow \infty} \frac{F^n(x)}{n} \quad (6.1)$$

It is possible to prove that the previous limit exists and it is independent of the choice of x used in the above calculation (see [39]). Moreover, such a limit is independent of the choice of lift (mod 1).

Definition 6.1.1. We say that

$$\lim_{n \rightarrow \infty} \frac{F^n(x)}{n} \pmod{1} := \text{rot}(f) \in \mathbb{R}/\mathbb{Z}$$

is the **rotation number** of f (see figure 6.2).

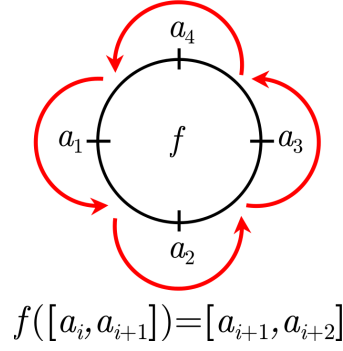


Figure 6.2: A homeomorphism with rotation number $\frac{1}{4}$.

Since the rotation number is independent of the choice of the lift, we will work with a preferred lift of elements and of functions. For any element $x \in S^1$ we denote by \widehat{x} the lift of x in $[0, 1)$. If $g \in \text{Homeo}_+(S^1)$ and the fixed point set $\text{Fix}(g) = \emptyset$, we denote by \widehat{g} the lift to $\text{Homeo}_+(\mathbb{R})$ such that $t < \widehat{g}(t) < t + 1$ for all $t \in \mathbb{R}$. If $g \in \text{Homeo}_+(S^1)$ and $\text{Fix}(g) \neq \emptyset$, we denote by \widehat{g} the lift to $\text{Homeo}_+(\mathbb{R})$ such that $\text{Fix}(\widehat{g}) \neq \emptyset$. We will use these definitions for lifts of elements and functions in Lemma 6.1.2(iv) and throughout the proof of Theorem 6.2.1. If we use this lift to compute the limit defined in (6.1), the result is always in $[0, 1)$. A proof of the next three results can be found in [39] and [45].

Lemma 6.1.2 (Properties of the Rotation Number). *Let $f, g \in \text{Homeo}_+(S^1)$, $G \leq \text{Homeo}_+(S^1)$ and k be a positive integer. Then:*

(i) $\text{rot}(f^g) = \text{rot}(f)$

(ii) $\text{rot}(f^k) = k \cdot \text{rot}(f)$

(iii) *If G is abelian then the map*

$$\begin{aligned} \text{rot} : G &\longrightarrow \mathbb{R}/\mathbb{Z} \\ f &\longmapsto \text{rot}(f) \end{aligned}$$

is a homomorphism

(iv) If $\text{rot}(g) = p/q \pmod{1} \in \mathbb{Q}/\mathbb{Z}$ and $s \in S^1$ is such that $g^q(s) = s$, then $\widehat{g^q}(\widehat{s}) = \widehat{s} + p$.

Two of the most important results about the rotation number are stated below.

Theorem 6.1.3 (Poincaré). *Let $f \in \text{Homeo}_+(S^1)$ be a homeomorphism. Then*

(i) *f has a periodic orbit of length q if and only if $\text{rot}(f) = p/q \pmod{1} \in \mathbb{Q}/\mathbb{Z}$ and p, q are coprime.*

(ii) *f has a fixed point if and only if $\text{rot}(f) = 0$.*

Theorem 6.1.4 (Denjoy). *Suppose $f \in \text{Homeo}_+(S^1)$ is piecewise-linear with finitely many breakpoints or is a C^1 homeomorphism whose first derivative has bounded variation. If the rotation number of f is irrational, then f is conjugate (by an element in $\text{Homeo}_+(S^1)$) to a rotation. Moreover, every orbit of f is dense in S^1 .*

The following is a standard result proved by Fricke and Klein (independently) which we will need in the proofs of section 6.2. Our citation is to a more recent proof in English.

Theorem 6.1.5 (Ping-Pong Lemma). *Let G be a group of permutations on a set X , let g_1, g_2 be elements of G of order at least three. If X_1 and X_2 are disjoint subsets of X and for all integers $n \neq 0, i \neq j, g_i^n(X_j) \subseteq X_i$, then g_1, g_2 freely generate the free group F_2 on two generators (see figure 6.3).*

Proof. See result 24 in section II.B of [26]. \square

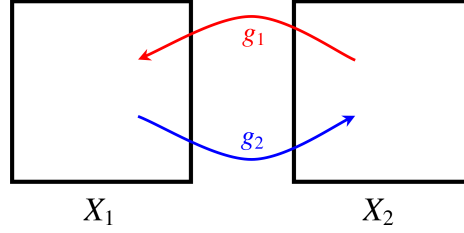


Figure 6.3: A graphical description of the ping pong lemma.

6.2 The Rotation Number Map is a Homomorphism

Our main goal for this section is to prove the following result.

Theorem 6.2.1. *Let $G \leq \text{Homeo}_+(S^1)$ with no non-abelian free subgroups. Then the rot map is a homomorphism.*

Before we begin with the proof of Theorem 6.2.1, we want to give a short account of its history. In his paper [47], Margulis proved a Theorem on the existence of G -invariant measures on S^1 which yields Theorem 6.2.1 as a corollary. Instead, we will give a direct proof of Theorem 6.2.1 and, in section 6.3, we will derive the original Theorem of Margulis. We notice that the statement of Theorem 6.2.1 does not hold in general: figure 6.4 shows two elements with rotation number 0 (hence they have fixed points) but whose product has no fixed points and must have non-zero rotation number.

Our proof divides naturally into several steps.

Lemma 6.2.2. *Let $f, g \in \text{Homeo}_+(S^1)$ such that $\text{Fix}(f) \neq \emptyset \neq \text{Fix}(g)$. If the intersection $\text{Fix}(f) \cap \text{Fix}(g) = \emptyset$, then $\langle f, g \rangle$ contains a non-abelian free subgroup. Equivalently, if $\langle f, g \rangle$ does not contain any non-abelian free subgroups, then $\text{Fix}(f) \cap \text{Fix}(g) \neq \emptyset$.*

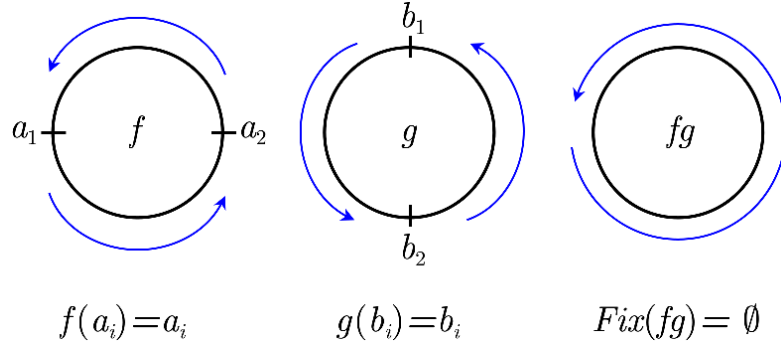


Figure 6.4: The rotation map is not a homomorphism in general.

Proof. Let $S^1 \setminus \text{Fix}(f) = \bigcup I_\alpha$ and $S^1 \setminus \text{Fix}(g) = \bigcup J_\beta$, for some suitable families of disjoint open intervals $\{I_\alpha\}, \{J_\beta\}$. By construction, $\partial I_\alpha \subseteq \text{Fix}(f)$ and $\partial J_\beta \subseteq \text{Fix}(g)$. We assume $\text{Fix}(f) \cap \text{Fix}(g) = \emptyset$ so that

$$S^1 \subseteq \left(\bigcup I_\alpha \right) \cup \left(\bigcup J_\beta \right).$$

Since S^1 is compact, we can write $S^1 = I_1 \cup \dots \cup I_r \cup J_1 \cup \dots \cup J_s$. Define $I = I_1 \cup \dots \cup I_r$ and $J = J_1 \cup \dots \cup J_s$. Since each $x \in \partial J$ lies in the interior of I , then there is an open neighborhood U_x of x such that $U_x \subseteq I$. Let $X_g = \bigcup_{x \in \partial J} U_x$. Similarly we build an open set X_f . If $x \in \partial J$, then the sequence $\{f^n(x)\}_{n \in \mathbb{N}}$ accumulates at a point of ∂I and so there is an $n \in \mathbb{N}$ such that $f^n(U_x) \subseteq X_f$. By repeating this process for each U_x , we can find a positive integer n_0 big enough so that $f^{n_0}(X_g) \cup f^{-n_0}(X_g) \subseteq X_f$. We act similarly on g and so we find an N big enough so that for all $m \geq N$ we have

$$f^m(X_g) \cup f^{-m}(X_g) \subseteq X_f, \quad g^m(X_f) \cup g^{-m}(X_f) \subseteq X_g.$$

If we define $g_1 = f^N, g_2 = g^N, X_1 = X_f, X_2 = X_g$, we have satisfied the hypothesis of Theorem 6.1.5 since both of the elements g_1, g_2 have infinite order. Thus $\langle g_1, g_2 \rangle$ is a non-abelian free subgroup of $\langle f, g \rangle$ (see figure 6.5 to see an example of two elements generating a free group). \square

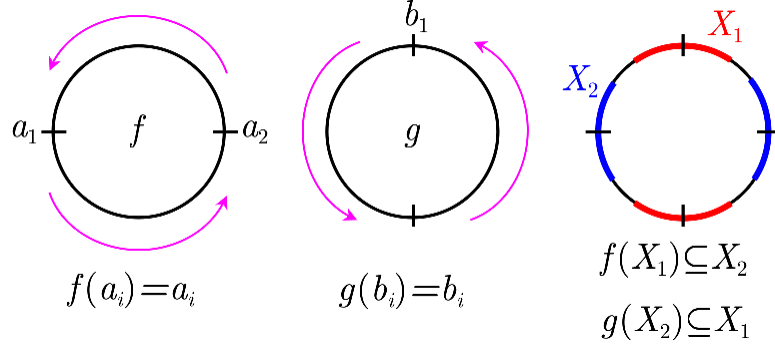


Figure 6.5: Two elements generating a free subgroup.

Corollary 6.2.3. *Let $f, g \in \text{Homeo}_+(S^1)$ such that $\text{Fix}(\widehat{f}) \neq \emptyset \neq \text{Fix}(\widehat{g})$. If $\text{Fix}(\widehat{f}) \cap \text{Fix}(\widehat{g}) = \emptyset$, then $\langle f, g \rangle$ contains a non-abelian free subgroup.*

If $G \leq \text{Homeo}_+(S^1)$ is a group, we define the set of homeomorphisms with fixed points

$$G_0 = \{g \in G \mid \exists s \in S^1, g(s) = s\} = \{g \in G \mid \text{rot}(g) = 0\} \subseteq G.$$

Corollary 6.2.4. *Let $G \leq \text{Homeo}_+(S^1)$ with no non-abelian free subgroups. The subset G_0 is a normal subgroup of $\text{Homeo}_+(S^1)$.*

Proof. Let $f, g \in G_0$ then, by Lemma 6.2.2, they must have a common fixed point, hence $fg^{-1} \in G_0$ and G_0 is a subgroup of G . Moreover, if $f \in G, g \in G_0$ and $s \in \text{Fix}(g)$, we have that $f^{-1}(s) \in \text{Fix}(f^{-1}gf)$ and so that $f^{-1}gf \in G_0$ and therefore G_0 normal. \square

If f has no fixed points then the support of f is the whole circle S^1 , otherwise the support can be broken into open intervals on which f is a one-bump function, that is $f(x) \neq x$ on them. Given $f \in \text{Homeo}_+(S^1)$, we define an *orbital* as an open component of the support of f .

The following three Lemmas can be derived using techniques similar to those of [9], however we give a direct proof of them.

Lemma 6.2.5. *Let $f, g \in \text{Homeo}_+(S^1)$ and let (a, b) be an orbital for f and (c, d) be an orbital for g such that $c < a < d < b$ (see figure 6.6). For every $\varepsilon > 0$, there are two integers M, N such that $f^M g^N$ has an orbital containing $(c + \varepsilon, b - \varepsilon)$.*

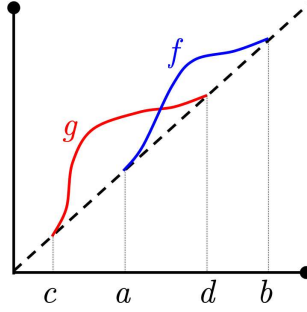


Figure 6.6: Intersecting bumps.

Proof. Without loss of generality we can assume that $c + \varepsilon < a$ and $b - \varepsilon > d$. There is an integer $N \neq 0$ such that $s := g^N(c + \varepsilon) > a$. Now choose a second integer $M \neq 0$ such that $f^M(s) > b - \varepsilon$. If $x \in (c + \varepsilon, b - \varepsilon)$, then $f^M g^N(x) > f^M g^N(c + \varepsilon) = f^M(s) > b - \varepsilon > x$, hence $f^M g^N$ has an orbital containing $(c + \varepsilon, b - \varepsilon)$. \square

Lemma 6.2.6. *Let $H \leq \text{Homeo}_+(S^1)$ and let (a, b) be an interval such that $\text{Fix}(H) \cap (a, b) = \emptyset$. For every $\varepsilon > 0$, there is an element $w \in H$ such that w has an orbital containing $(a + \varepsilon, b - \varepsilon)$.*

Proof. We fix a point $c \in (a, b)$ and an $\varepsilon > 0$. We define the following notation: let \mathcal{J} be the family of elements of H that do not fix c . The set \mathcal{J} is non-empty, since $c \notin \text{Fix}(H)$. For any element of $h \in \mathcal{J}$, let $O(h)$ denote the orbital of h containing c and let $l(h)$ and $r(h)$ respectively be the left and right endpoints of $O(h)$.

Claim 1. The following supremum of all right endpoints of elements in \mathcal{N}

$$R := \sup_{h \in \mathcal{J}} \{r(h)\} \geq b.$$

Proof. Assume, by contradiction, that $R < b$. Since $R \notin \text{Fix}(H)$, there is an $f \in H$ with an orbital (s, t) containing R and we can assume that $f(x) > x$, for all $x \in (s, t)$. By definition of R , there is an element $g \in \mathcal{J}$ with an orbital $O(g)$ such that its right endpoint $r(g) > s$. If $s \leq l(g)$, then $f \in \mathcal{J}$ and its right endpoint is bigger than R , which is not possible. Hence we must have $l(g) < s < r(g) < t$ and we can apply Lemma 6.2.5 to find an element $f^M g^N$ with an orbital containing $(l(g) + \delta, t - \delta)$ and with δ chosen to be small enough that $c, R \in (l(g) + \delta, t - \delta)$. This would imply that $f^M g^N \in \mathcal{J}$ and its right endpoint is bigger than R , which is a contradiction to the definition of supremum. \square

Thus we must have $R \geq b$ and so the family \mathcal{J} has elements with “large” orbitals on the right. We will now extend this procedure to make them “large” on the left. We define the following new subfamily of elements of \mathcal{J}

$$\mathcal{K} = \{h \in \mathcal{J} \mid r(h) > b - \varepsilon\}$$

By Claim 1, the family \mathcal{K} is non-empty.

Claim 2. The following infimum of all right endpoints of elements in \mathcal{K}

$$L := \inf_{h \in \mathcal{K}} \{l(h)\} \leq a.$$

Proof. We repeat the idea of the previous Claim, by assuming that $L > a$ and then finding two elements f, g on which we can apply Lemma 6.2.5. \square

By Claim 2, we can choose an element $w \in \mathcal{K}$ that has an orbital with $l(w) < a + \varepsilon$.

By definition of \mathcal{K} , w satisfies the thesis. \square

Lemma 6.2.7. *Let $H \leq \text{Homeo}_+(S^1)$ and let $(a_1, b_1), \dots, (a_r, b_r)$ be disjoint intervals such that*

$$\text{Fix}(H) \cap \left(\bigcup_{i=1}^r (a_i, b_i) \right) = \emptyset.$$

For every $\varepsilon > 0$, there is an element $w \in H$ such that, the element w has a support containing $(a_i + \varepsilon, b_i - \varepsilon)$, for each $i = 1, \dots, r$.

Proof. By induction on the number of intervals r . The case $r = 1$ has been proven in Lemma 6.2.6. We assume the result holds for the $r - 1$ intervals $(a_1, b_1), \dots, (a_{r-1}, b_{r-1})$. Define the family of elements

$$\mathcal{J} = \left\{ h \in H \mid \text{supp}(h) \supseteq \bigcup_{i=1}^{r-1} [a_i + \varepsilon, b_i - \varepsilon] \right\}$$

By induction hypothesis, the family \mathcal{J} is non-empty. We also observe that $\text{supp}(h)$ is always an open set, hence it is a union of intervals that contains the closed set $\bigcup_{i=1}^{r-1} [a_i + \varepsilon, b_i - \varepsilon]$ properly. We fix a point $c \in (a_r, b_r)$. We now want to prove that \mathcal{J} contains elements that do not fix c .

Claim. The following subfamily of \mathcal{J} :

$$\mathcal{K} = \left\{ h \in \mathcal{J} \mid h(c) \neq c \right\} \neq \emptyset.$$

Proof. Let $f \in \mathcal{J}$. If $f(c) \neq c$, we are done. Otherwise, suppose that $f(c) = c$. Since $c \notin \text{Fix}(H)$, there is a $g \in H$ such that $g(c) \neq c$. For each $i = 1, \dots, r - 1$ consider the interval (s_i, t_i) of the support of f containing $[a_i + \varepsilon, b_i - \varepsilon]$ properly. On each (s_i, t_i) we have two cases: (i) an orbital of g contains s_i or t_i , so we can apply Lemma 6.2.5 to find integers M_i, N_i such that $f^{M_i} g^{N_i}$ has an orbital containing $[a_i + \varepsilon, b_i - \varepsilon]$, or (ii) an orbital of g contains (s_i, t_i) properly and again we can find powers M_i, N_i such that $f^{M_i} g^{N_i}$ has an orbital containing $[a_i + \varepsilon, b_i - \varepsilon]$ (see figure 6.7). If we now take $M = \max\{M_1, \dots, M_{r-1}\}$ and $N = \max\{N_1, \dots, N_{r-1}\}$, we have that $f^M g^M \in \mathcal{J}$ and, by construction, $f^M g^N \in \mathcal{J}$. \square

The proof now proceeds as in Lemma 6.2.6. We first find elements with orbitals whose right endpoint is near b_r and then do the same on the left. As done in the previous Claim, this procedure can be followed so that the support of the families of elements always contain properly the union $\bigcup_{i=1}^{r-1} [a_i + \varepsilon, b_i - \varepsilon]$. \square

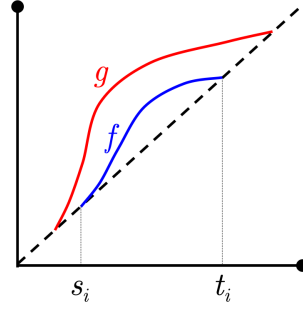


Figure 6.7: Non-intersecting bumps.

Lemma 6.2.8 (Finite Intersection Property). *Let $G \leq \text{Homeo}_+(S^1)$ with no non-abelian free subgroups. Then the family $\{\text{Fix}(g) \mid g \in G_0\}$ satisfies the finite intersection property, i.e. for all n -tuples $g_1, \dots, g_n \in G_0$, we have $\text{Fix}(g_1) \cap \dots \cap \text{Fix}(g_n) \neq \emptyset$.*

Proof. We use induction on n , with the case $n = 2$ being true by Lemma 6.2.2. We assume that the result is true for any $(n - 1)$ -tuple of elements in G_0 . Let $g_1, \dots, g_n \in G_0$ and assume, by contradiction, that $\text{Fix}(g_1) \cap \dots \cap \text{Fix}(g_n) = \emptyset$. Let $H = \langle g_1, \dots, g_{n-1} \rangle$ and notice that $\text{Fix}(H) \neq \emptyset$ by induction hypothesis. Write $S^1 \setminus \text{Fix}(H) = \bigcup I_\alpha$ and $S^1 \setminus \text{Fix}(g_r) = \bigcup J_\beta$, for some suitable families of open intervals $\{I_\alpha\}, \{J_\beta\}$. By construction, $\partial I_\alpha \subseteq \text{Fix}(H)$ and $\partial J_\beta \subseteq \text{Fix}(g_r)$. Since $\text{Fix}(H) \cap \text{Fix}(g_r) = \emptyset$ we have

$$S^1 \subseteq \left(\bigcup I_\alpha \right) \cup \left(\bigcup J_\beta \right).$$

Since S^1 is compact, we can write $S^1 = I_1 \cup \dots \cup I_r \cup J_1 \cup \dots \cup J_s$ and notice that $\text{Fix}(g_r) \subseteq \bigcup_{i=1}^r I_i$. Since the intersection $\text{Fix}(H) \cap \left(\bigcup_{m=1}^s J_m \right) = \emptyset$. If $I_i = (a_i, b_i)$

we apply Lemma 6.2.6 to build an element $w \in H$ such that w has an orbital containing $(a_i + \varepsilon, b_i - \varepsilon)$, for every $i = 1, \dots, r-1$. We can choose $\varepsilon > 0$ to be small enough so $\text{Fix}(g_r) \subseteq \bigcup_{i=1}^r (a_i + \varepsilon, b_i - \varepsilon) \subseteq \text{supp}(w)$ thus implying that $\text{Fix}(w) \cap \text{Fix}(g_r) = \emptyset$. We can again apply Lemma 6.2.2 to build a non-abelian free group inside $\langle w, g_n \rangle$, contradicting the assumption on G . Thus, for every finite set $H \subset G_0$, we have

$$\bigcap_{h \in H} \text{Fix}(h) \neq \emptyset$$

which proves that the family $\{\text{Fix}(g) \mid g \in G_0\}$ has the finite intersection property. \square

Corollary 6.2.9. *Let $G \leq \text{Homeo}_+(S^1)$ with no non-abelian free subgroups. The subgroup G_0 admits a global fixed point, i.e. $\text{Fix}(G_0) \neq \emptyset$.*

Proof. By the previous Lemma we have that the family $\{\text{Fix}(g) \mid g \in G_0\}$ has the finite intersection property. By compactness of the unit circle S^1 we have that:

$$\text{Fix}(G_0) = \bigcap_{g \in G_0} \text{Fix}(g) \neq \emptyset. \quad \square$$

In order to prove Theorem 6.2.1 we observe that the element $(fg)^k$ can be rewritten $f^k g^k h_k$ for some suitable product of commutators $h_k \in [G, G]$. If we prove that every element $[G, G]$ has a global fixed point s we can compute the rotation number on s , so that $(fg)^k(s) = f^k g^k$. We will prove that this is indeed the case.

Lemma 6.2.10. *Let $G \leq \text{Homeo}_+(S^1)$ and let $f, g \in G$. Suppose one of the following two cases is true:*

- (i) G has no non-abelian free subgroups and $\text{rot}(f) = \text{rot}(g) \in \mathbb{Q}/\mathbb{Z}$, or
- (ii) $\text{rot}(f) = \text{rot}(g) \notin \mathbb{Q}/\mathbb{Z}$.

Then $fg^{-1} \in G_0$.

Proof. (i) Assume $\text{rot}(f) = \text{rot}(g) = k/m \in \mathbb{Q}/\mathbb{Z}$ with k, m positive integers and that G has no non-abelian free subgroups. Moreover, f^m and g^m have fixed points in S^1 and $\widehat{f^m}(\widehat{x}) = \widehat{x} + k$ and $\widehat{g^m}(\widehat{y}) = \widehat{y} + k$, for any $x \in \text{Fix}(f^m), y \in \text{Fix}(g^m)$ by Lemma 6.1.2(iv). Thus f^m and g^m must have a common fixed point $s \in S^1$ by Lemma 6.2.2. We argue, by contradiction, that $fg^{-1} \notin G_0$, so that $\widehat{f} > \widehat{g}$ or $\widehat{f} < \widehat{g}$. Suppose the former so $\widehat{f^m} > \widehat{g^m}$, but this is impossible as $\widehat{f^m}(\widehat{s}) = \widehat{s} + k = \widehat{g^m}(\widehat{s})$.

(ii) Assume now that $\text{rot}(f) = \text{rot}(g) \notin \mathbb{Q}/\mathbb{Z}$. Again, we argue by contradiction that $fg^{-1} \notin G_0$ and we suppose $\widehat{f} > \widehat{g}$. We observe that, for any map $h \in \text{Homeo}_+(S^1)$ such that $\widehat{f} \geq \widehat{h} \geq \widehat{g}$, we have $\text{rot}(f) \geq \text{rot}(h) \geq \text{rot}(g) = \text{rot}(f)$ and so $\text{rot}(h) \notin \mathbb{Q}/\mathbb{Z}$. By compactness of S^1 and the fact that $\widehat{f} > \widehat{g}$, we can find an $h \in \text{PL}_+(S^1)$ such that $\widehat{f} > \widehat{h} > \widehat{g}$. We use Denjoy's theorem on h to find $z \in \text{Homeo}(S^1)$ such that h^z is a rotation. Therefore $\widehat{h^z}$ is a straight line $t \rightarrow t + \text{rot}(g)$. Now since $\widehat{f^z} > \widehat{h^z}$, we can find a rotation $u \in \text{Homeo}(S^1)$ such that its lift is a straight line $\widehat{u} : t \rightarrow t + \text{rot}(u)$ with $\text{rot}(u) > \text{rot}(h)$ and $\widehat{f^z} > \widehat{u} > \widehat{h^z}$. (see figure 6.8). To conclude we observe that

$$\text{rot}(f) = \text{rot}(f^z) \geq \text{rot}(u) > \text{rot}(h^z) = \text{rot}(h) = \text{rot}(f)$$

yielding a contradiction. \square

Corollary 6.2.11. *Let $G \leq \text{Homeo}_+(S^1)$ with no non-abelian free subgroups, then we have $[G, G] \leq G_0$.*

Corollary 6.2.12. *Let $G \leq \text{Homeo}_+(S^1)$ with no non-abelian free subgroups. Suppose that every element of $G \setminus \{id\}$ has no fixed points. Then G is abelian.*

Corollary 6.2.12 is true in a greater generality. In fact, Theorem 6.5.2 proves it without any requirement on the subgroups of G .

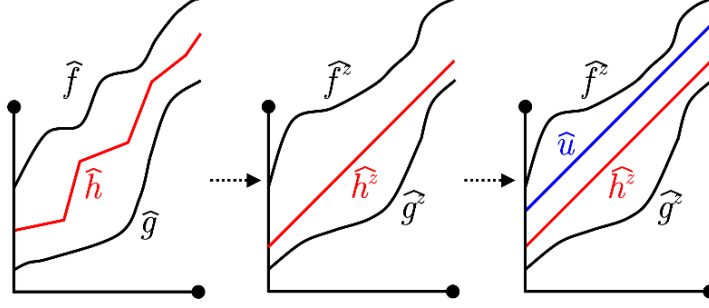


Figure 6.8: Making room for straight lines between \widehat{f} and \widehat{g} .

Lemma 6.2.13. *Let $G \leq \text{Homeo}_+(S^1)$ with no non-abelian free subgroups. Let $f, g \in G$ and $s \in S^1$ be a fixed point of $[f, g]$. Then \widehat{s} is a fixed point for $[U, V]$, for any U lift of f and V lift of g in $\text{Homeo}_+(\mathbb{R})$.*

Proof. If $T(x) = x + 1$ then $U = T^m \widehat{f}$ and $V = T^n \widehat{g}$ for some suitable integers m, n . Moreover, it is immediate to verify that

$$[U, V](x) = [\widehat{f}, \widehat{g}](x), \forall x \in \mathbb{R}.$$

Thus, we need only to prove that $[\widehat{f}, \widehat{g}](\widehat{s}) = \widehat{s}$. We divide the proof into two cases.

Case 1: $\text{Fix}(\widehat{f}) = \emptyset = \text{Fix}(\widehat{g})$. We have that $t < \widehat{f}(t) < t + 1$ and $t < \widehat{g}(t) < t + 1$ for all $t \in \mathbb{R}$. Since $fg(s) = gf(s)$ we also have $k := \widehat{f}\widehat{g}(s) - \widehat{g}\widehat{f}(s) \in \mathbb{Z}$. If $\widehat{f}\widehat{g}(s) \geq \widehat{g}\widehat{f}(s)$ then, since \widehat{g} is increasing and $\widehat{s} < \widehat{f}(\widehat{s})$, we have $\widehat{g}\widehat{f}(\widehat{s}) > \widehat{g}(\widehat{s})$ and so

$$|k| = \widehat{f}\widehat{g}(s) - \widehat{g}\widehat{f}(s) \leq \widehat{f}\widehat{g}(s) - \widehat{g}(\widehat{s}) < 1$$

implying that $k = 0$. A similar argument holds if $\widehat{f}\widehat{g}(s) \leq \widehat{g}\widehat{f}(s)$.

Case 2: $\text{Fix}(\widehat{f}) \neq \emptyset$ or $\text{Fix}(\widehat{g}) \neq \emptyset$. We can assume that $\text{Fix}(\widehat{f}) \neq \emptyset$. Then also $\text{Fix}(\widehat{g}^{-1}\widehat{f}\widehat{g}) \neq \emptyset$. By Corollary 6.2.3 we must have $\text{Fix}(\widehat{f}) \cap \text{Fix}(\widehat{g}^{-1}\widehat{f}\widehat{g}) \neq \emptyset$ and so

this implies that $[\widehat{f}, \widehat{g}]$ intersects the diagonal. Since $[f, g](s) = s$, then $[\widehat{f}, \widehat{g}](\widehat{s}) = \widehat{s}$. \square

Now we are ready to prove the main theorem of this section.

Proof of Theorem 6.2.1. Let $f, g \in G$. We write the power $(fg)^k = f^k g^k h_k$ where h_k is a suitable product of commutators used to shift the f 's and g 's to the left. Since $h_k \in [G, G] \leq G_0$ for all positive integers k then, if $s \in S^1$ is a global fixed point for G_0 , we have $h_k(s) = s$. Similarly, we observe that $(\widehat{f}\widehat{g})^k = \widehat{f}^k \widehat{g}^k H_k$ where H_k is a suitable product of commutators and H_k is a lift for h_k . By Lemma 6.2.13 we must have that $H_k(\widehat{s}) = \widehat{s}$ for all positive integers k . Thus we observe that:

$$(\widehat{f}\widehat{g})^n(\widehat{s}) = \widehat{f}^n \widehat{g}^n H_n(\widehat{s}) = \widehat{f}^n \widehat{g}^n(\widehat{s}).$$

We now find upper and lower bounds for $\widehat{f}^n \widehat{g}^n(\widehat{s})$. Observe that, for any two real numbers a, b we have that

$$\widehat{f}^n(a) + b - 1 < \widehat{f}^n(a) + \lfloor b \rfloor \leq \widehat{f}^n(a + b) < \widehat{f}^n(a) + \lfloor b \rfloor + 1 \leq \widehat{f}^n(a) + b + 1$$

where $\lfloor \cdot \rfloor$ denotes the floor function. By applying this inequality to $\widehat{f}^n \widehat{g}^n(\widehat{s}) = \widehat{f}^n(\widehat{s} + (\widehat{g}^n(\widehat{s}) - \widehat{s}))$ we get

$$\widehat{f}^n(\widehat{s}) + \widehat{g}^n(\widehat{s}) - \widehat{s} - 1 \leq \widehat{f}^n(\widehat{s} + (\widehat{g}^n(\widehat{s}) - \widehat{s})) \leq \widehat{f}^n(\widehat{s}) + \widehat{g}^n(\widehat{s}) - \widehat{s} + 1.$$

We divide the previous inequalities by n , and get

$$\frac{\widehat{f}^n(\widehat{s}) + \widehat{g}^n(\widehat{s}) - \widehat{s} - 1}{n} \leq \frac{(\widehat{f}\widehat{g})^n(\widehat{s})}{n} \leq \frac{\widehat{f}^n(\widehat{s}) + \widehat{g}^n(\widehat{s}) - \widehat{s} + 1}{n}.$$

By taking the limit for $n \rightarrow \infty$ of the previous expression, we immediately obtain $\text{rot}(fg) = \text{rot}(f) + \text{rot}(g)$. \square

Corollary 6.2.14. *Let $G \leq \text{Homeo}_+(S^1)$ with no non-abelian free subgroups. Then $\text{rot} : G \rightarrow \mathbb{R}/\mathbb{Z}$ is a group homomorphism and*

$$(i) \ker(\text{rot}) = G_0,$$

$$(ii) G/G_0 \cong \text{rot}(G).$$

$$(iii) \text{ for all } f, g \in G, fg^{-1} \in G_0 \text{ if and only if } \text{rot}(f) = \text{rot}(g).$$

6.3 Applications: Margulis' Theorem

In this section we show how the techniques developed in Section 6.2 yield two known results for groups of homeomorphisms of the unit circle.

Theorem 6.3.1 (Margulis, [47]). *Let $G \leq \text{Homeo}_+(S^1)$. Then at least one of the two following statements must be true:*

(i) *G has a non-abelian free subgroup, or*

(ii) *there is a G -invariant probability measure on S^1 .*

Proof. We assume that (i) does not hold. The proof must be divided into two cases.

Case 1: G/G_0 is finite. Let $s \in \text{Fix}(G_0)$ and consider the finite orbit s^G . Then for every subset $X \subseteq S^1$ assign

$$\mu(X) = \frac{\# s^G \cap X}{\# s^G}.$$

This obviously defines a probability measure on S^1 .

Case 2: G/G_0 is infinite and therefore $\text{rot}(G)$ is dense in \mathbb{R}/\mathbb{Z} . Fix $s \in \text{Fix}(G_0)$ as an origin and write S^1 as $[0, 1]$. We regard s^G as a subset of $[0, 1]$ and define the map $\varphi : s^G \rightarrow \text{rot}(G)$, given by $\varphi(s^g) = \text{rot}(g)$, for any $g \in G$. It is immediate that

φ is well-defined and order-preserving. We take the “closure” of this map, by defining

$$\begin{aligned}\bar{\varphi} : [0, 1] &\longrightarrow [0, 1] \\ a &\longmapsto \sup\{rot(g) \mid s^g \leq a, g \in G\}.\end{aligned}$$

By construction, the map $\bar{\varphi}$ is order-preserving. Moreover, since the image of $\bar{\varphi}$ contains $rot(G)$, it is dense in $[0, 1]$. Since $\bar{\varphi}$ is an order-preserving map whose image is dense in $[0, 1]$, then $\bar{\varphi}$ is a continuous map. This allows us to define the Lebesgue-Stieltjes measure associated to $\bar{\varphi}$ on the Borel algebra of S^1 (see [46]), that is, for every half-open interval $(a, b] \subseteq S^1$ we define

$$\mu((a, b]) := \bar{\varphi}(b) - \bar{\varphi}(a).$$

Since the map rot is a homomorphism, it is straightforward to see that the measure μ is G -invariant. For example, consider an interval $(s^{g_1}, s^{g_2}]$ such that $rot(g_1) \leq rot(g_2) < 1$ (that is, neither s^{g_1} nor s^{g_2} wrap around the circle and pass s). If $g \in G$, we have that

$$\mu(s^{gg_1}, s^{gg_2}] = rot(gg_2) - rot(gg_1) = rot(g) + rot(g_2) - rot(g) - rot(g_1) = \mu(s^{g_1}, s^{g_2}]$$

The other cases are dealt similarly, by doing additions and subtractions in \mathbb{R}/\mathbb{Z} . The same can be verified for any other half-open interval. By definition of the measure, $\mu(S^1) = 1$ and $\mu(p) = 0$, for every point $p \in S^1$, and we are done. \square

The following result is strongly believed to be well known, but unfortunately we were unable to find a reference for it.

Theorem 6.3.2. *Suppose G is a subgroup of $\text{Homeo}_+(S^1)$ which contains no non-abelian free subgroups, and there is an element $g \in G$ such that*

(i) $rot(g) \notin \mathbb{Q}/\mathbb{Z}$, and

(ii) g is piecewise-linear with finitely many breakpoints, or C^1 with bounded variation in its first derivative,

then G is topologically conjugate to a group of rotations. In particular, G is abelian.

Proof. By Denjoy's Theorem 6.1.4 the orbits of g are dense in S^1 . Suppose there is $id \neq h \in G_0$ and let $s \in \text{Fix}(G_0)$. Then $g(s) \in \text{Fix}(h)$ in fact

$$h(g(s)) = gg^{-1}hg(s) = g(h^g(s)) = g(s)$$

since $h^g \in G_0 \trianglelefteq G$. Thus h must fix the sequence of points $\{g^k(s)\}$, which is dense in S^1 and so h must fix the whole S^1 , giving a contradiction, since $h \neq id$. Thus $\text{Fix}(G_0) = S^1$ and so G_0 is trivial. By Corollary 6.2.14 we have $G \cong G/G_0 \cong \text{rot}(G) \leq \mathbb{R}/\mathbb{Z}$. By Denjoy's Theorem 6.1.4, there is a $z \in \text{Homeo}_+(S^1)$ such that g^z is a rotation. Thus $G^z \leq C_{\text{Homeo}_+(S^1)}(g^z) = \{\text{all rotations}\}$. \square

6.4 Structure and Embedding Theorems

We start the section with a result which classifies the structure of subgroups of $\text{Homeo}_+(S^1)$ with no non-abelian free subgroups. We consider an orbit s^G of a point s of $\text{Fix}(G_0)$ under the action of G (so that any of the points of the closure $\overline{s^G} \subseteq \text{Fix}(G_0)$), then we choose a fundamental domain D for the action of G on $S^1 \setminus \overline{O(x)}$. Since $S^1 \setminus \overline{s^G}$ is open, the fundamental domain will be given by a union of intervals. By restricting G_0 to this fundamental domain and we get a group H_0 which acts as a set of homeomorphisms of a disjoint union of intervals. We will prove that G is isomorphic to the wreath structure of G/G_0 over the group H_0 which acts on the fundamental domain.

Theorem 6.4.1. *Let $G \leq \text{Homeo}_+(S^1)$ with no non-abelian free subgroups. Then:*

(i) *G is abelian, or*

(ii) *$G \hookrightarrow H_0 \wr T$, the standard unrestricted wreath product, where $T := G/G_0$ is isomorphic to a countable subgroup of \mathbb{R}/\mathbb{Z} and $H_0 \leq \prod \text{Homeo}_+(I_i)$ has no non-abelian free subgroups.*

Remark 6.4.2. If $G \leq \text{PL}_+(S^1)$ is non-abelian, then $T \leq \mathbb{Q}/\mathbb{Z}$ because of Denjoy's Theorem. This is also a consequence of Theorem 6.3.2.

Proof. (i) If $G_0 = \{id\}$ then $G \cong G/G_0 \cong \text{rot}(G) \leq \mathbb{R}/\mathbb{Z}$. (ii) Suppose G_0 non-trivial, so that $\text{Fix}(G_0) \neq S^1$ and define $T = G/G_0$. Let $s \in \text{Fix}(G_0)$ and consider the open subset $S^1 \setminus \overline{s^T}$, where s^T is the orbit of s under the action of T . The set $S^1 \setminus \overline{s^T}$ is a collection of, at most countably many, disjoint open intervals. We can define a fundamental domain for the action of T on $S^1 \setminus \overline{s^T}$ as the union $D = \bigcup_{i \in I} I_i$ of a collection $\{I_i\}_{i \in I}$ of at most countably many intervals I_i such that

$$t_1(D) \cap t_2(D) = \emptyset, \quad t_1 \neq t_2,$$

$$S^1 \setminus \overline{s^T} = \bigcup_{t \in T} t(D)$$

Claim 1: The fundamental domain D exists.

Proof of Claim 1. Let T act on $S^1 \setminus \overline{s^T}$ and consider two intervals I_1, I_2 to be equivalent if there is $t \in T$ such that $t(I_1) = I_2$. For each equivalence class C_i , we apply the Axiom of Choice to choose an interval I_i representing the class. We define D to be the union of these representatives. \square

Since $\overline{s^T} \subseteq \text{Fix}(G_0)$ we have

$$S^1 \setminus \bigcup_{t \in T} t(D) \subseteq \text{Fix}(G_0).$$

Claim 2: Define $H_0 := G_0|_D$ restriction of G_0 to D . Then there is an embedding $H'_0 = G_0|_{t^{-1}(D)} \hookrightarrow \prod_{i \in \mathcal{I}} \text{Homeo}_+(t^{-1}(I_i))$. In particular, $H_0 \hookrightarrow \prod_{i \in \mathcal{I}} \text{Homeo}_+(I_i)$.

Proof of Claim 2. This is immediate, once we observe that if $h \in H_0$ and $t \in G \setminus G_0$, then $t^{-1}ht(t^{-1}(D)) = t^{-1}(D)$, since G_0 fixes the endpoints of the intervals I_i . \square

It is important to notice that H_0 is not necessarily contained in G_0 , since H_0 has its support in D , while an element of G_0 has support in $\bigcup_{t \in T} t(D)$. From Claim 2 it is now obvious that there is an embedding

$$\varphi : G_0 \hookrightarrow \prod_{t \in T} H'_0 = \prod_{t \in T} \prod_{i \in \mathcal{I}} \text{Homeo}_+(t^{-1}(I_i))$$

We observe $\prod_{t \in T} H'_0 \cong \langle H'_0 | t \in T \rangle \leq \text{Homeo}_+(S^1)$ and we define $H := \langle H'_0 | t \in T \rangle$ and

$$E := \langle G, H'_0 | t \in T \rangle \leq \text{Homeo}_+(S^1).$$

By definition of E we get the following exact sequence

$$1 \rightarrow H \xrightarrow{i} E \xrightarrow{\pi} E/H \rightarrow 1$$

where i is the inclusion map and π is the natural projection $\pi : E \rightarrow E/H$. Notice that $E/H \cong G/(G \cap H)$ and $G \cap H \leq G_0$, by definition of G_0 . By the argument above $G_0 \leq H$ and so $G \cap H = G_0$ thus implying that $E/H \cong G/G_0 = T$, so we can rewrite the sequence as

$$1 \rightarrow H \xrightarrow{i} E \xrightarrow{\pi} T \rightarrow 1$$

where T acts on the base group by shifts.

Claim 3: $E \cong E_0 := H_0 \wr T$

Proof of Claim 3. By a standard result in cohomology of groups (see Theorem 11.4.10 in [55]), if we can prove that $H^2(T, Z(\prod H'_0)) = 0$ (where $Z(\prod H'_0)$ denotes the center of $\prod H'_0$), there can be only one possible extension of $\prod H'_0$ by T . We observe that $H_0 \wr T$ is one such extension, so it suffices to prove that $H^2(T, Z(\prod H'_0)) = 0$ to show that any other extension will be equivalent to the wreath product $H_0 \wr T$. We use Shapiro's Lemma to compute this cohomology group (see Proposition 6.2 in [20]). We have

$$\begin{aligned} H^2(T, Z(\prod H'_0)) &= H^2(T, \prod Z(H_0)^t) = \\ &= H^2(T, \text{Coind}_{\{id\}}^T Z(H_0)) = H^2(\{id\}, Z(H_0)) = 0. \quad \square \end{aligned}$$

Remark 6.4.3. We observe that the wreath product in the previous result is unrestricted, because the elements of $\text{Homeo}_+(S^1)$ can have infinitely many bumps and so the elements of G_0 may be non-trivial on infinitely many intervals. Conversely, if we assume $G \leq \text{PL}_+(S^1)$, this would imply that any element in G_0 is non-trivial only at finitely many intervals, and so that G_0 can be embedded in the direct sum \bigoplus . This argument explains why the wreath products in the following Theorem 6.4.5 is unrestricted and the ones in Theorems 6.4.7 and 6.4.8 are restricted.

Remark 6.4.4. We notice that, in the statement of the previous Theorem, we may replace the conclusion " $H_0 \leq \prod \text{Homeo}_+(I_i)$ " with $H_0 \leq \text{Homeo}_+(I)$, because we can always build an embedding $\prod \text{Homeo}_+(I_i) \hookrightarrow H_0$.

We now turn to prove existence results and show that subgroups with wreath product structure do exist in $\text{Homeo}_+(S^1)$ and in $\text{PL}_+(S^1)$.

Theorem 6.4.5. *For every $T \leq \mathbb{R}/\mathbb{Z}$ countable and for every $H_0 \leq \text{Homeo}_+(I)$*

there is an embedding $H_0 \wr T \hookrightarrow \text{Homeo}_+(S^1)$, where the wreath product $H_0 \wr T = (\prod H_0) \rtimes T$ is unrestricted.

Proof. We divide the proof into two cases: T infinite and T finite. If T is infinite, we enumerate the elements of $T = \{t_1, \dots, t_n, \dots\}$ and we build a sequence:

$$\frac{1}{2}, \frac{1}{2^2}, \dots, \frac{1}{2^n}, \dots$$

We identify S^1 with the interval $[0, 1]$ to fix an origin and an orientation of the unit circle. T is countable subgroup of \mathbb{R}/\mathbb{Z} , so it is non-discrete and therefore it is dense in S^1 . Now define the following map:

$$\begin{aligned} \varphi : [0, 1] = S^1 &\longrightarrow [0, 1] = S^1 \\ x &\longmapsto \sum_{t_i < x} \frac{1}{2^i} \end{aligned}$$

(where $t_i < x$ is written with respect to the order in $[0, 1]$). It is immediate from the definition to see that the map is order-preserving and it is injective, when restricted to T . Observe now that

$$\begin{aligned} \varphi(t_1) &= \sum_{t_i < t_1} \frac{1}{2^i} \\ \varphi(t_1 + \varepsilon) &= \sum_{t_i < t_1 + \varepsilon} \frac{1}{2^i} \end{aligned}$$

If we let $\varepsilon \rightarrow 0$, we see

$$\alpha := \varphi(t_1) \leq \varphi(t_1 + \varepsilon) \xrightarrow{\varepsilon \rightarrow 0} \sum_{t_i \leq t_1} \frac{1}{2^i} = \alpha + \frac{1}{2}$$

Since φ is order-preserving, we have $(\alpha, \alpha + \frac{1}{2}) \cap \varphi(T) = \emptyset$. More generally, it can be seen that

$$\bigcup_{i \in \mathbb{N}} \left(\varphi(t_i), \varphi(t_i) + \frac{1}{2^i} \right) \cap \overline{\varphi(T)} = \emptyset$$

Claim. The unit circle can be written as the disjoint union

$$S^1 = \bigcup_{i \in \mathbb{N}} \left(\varphi(t_i), \varphi(t_i) + \frac{1}{2^i} \right) \cup \overline{\varphi(T)}.$$

Proof of Claim. Let $X = \bigcup_{i \in \mathbb{N}} \left(\varphi(t_i), \varphi(t_i) + \frac{1}{2^i} \right)$ and let $x_0 \notin X$. We want to prove that, for any $\varepsilon > 0$, there is a $t_\varepsilon \in T$ such that $x_0 - \varepsilon < \varphi(t_\varepsilon) < x_0$: thus if we take $\varepsilon_n = \frac{1}{n}$, we can find a sequence $t_{\varepsilon_n} \in T$ such that $\varphi(t_{\varepsilon_n}) \rightarrow x_0$ and so $x_0 \in \overline{\varphi(T)}$.

Assume, by contradiction, that there is an $\varepsilon > 0$ such that $\varphi(t) \notin (x_0 - \varepsilon, x_0)$, for any $t \in T$. Observe that $(x_0 - \varepsilon, x_0) \cap A = \emptyset$. If this were not true, there would be a $t_i \in T$ such that $(x_0 - \varepsilon, x_0) \cap \left(\varphi(t_i), \varphi(t_i) + \frac{1}{2^i} \right) \neq \emptyset$. We have the following three cases:

- $\varphi(t_i) \in (x_0 - \varepsilon, x_0)$. This is impossible, because of the definition of $(x_0 - \varepsilon, x_0)$.
- $\varphi(t_i) + \frac{1}{2^i} \in (x_0 - \varepsilon, x_0)$. Let $\{t_{i_r}\} \subseteq T$ be a decreasing sequence converging to t_i^+ , then $\lim_{r \rightarrow \infty} \varphi(t_{i_r}) = \varphi(t_i) + \frac{1}{2^i}$. Thus there is an r such that $\varphi(t_{i_r}) \in (x_0 - \varepsilon, x_0)$, contradicting the assumption on $(x_0 - \varepsilon, x_0)$ so this case is not possible.
- $(x_0 - \varepsilon, x_0) \subseteq \left(\varphi(t_i), \varphi(t_i) + \frac{1}{2^i} \right)$. This is also impossible, as it would imply that $x_0 \in \left(\varphi(t_i), \varphi(t_i) + \frac{1}{2^i} \right) \subseteq A$.

Thus $(x_0 - \varepsilon, x_0) \cap A = \emptyset$ and so

$$1 = m([0, 1]) \geq m((x_0 - \varepsilon, x_0)) + m(A) = \varepsilon + 1 > 1$$

where m is the Lebesgue measure on $[0, 1]$. Hence we have a contradiction and the Claim is proved. \square

We can visualize the set $C := \overline{\varphi(T)}$ as a Cantor set. If we regard $[0, 1]$ as S^1 , then the group T acts on $[0, 1]$ by rotations and so each $t \in T$ induces a map $t : C \rightarrow C$. Now we extend this map to a map $t : S^1 \rightarrow S^1$ by sending an interval $X_i := \left[\varphi(t_i), \varphi(t_i) + \frac{1}{2^i} \right] \subseteq S^1 \setminus C$ linearly onto the interval $t(X_i) := \left[\varphi(t_j), \varphi(t_j) + \frac{1}{2^j} \right]$, where $t_j = t + t_i$ according to the enumeration of T . Thus we can identify T as a subgroup of $\text{Homeo}_+(S^1)$.

We stretch the interval I into $\overline{X_1}$ and we can regard the group H_0 as a subgroup of $\{g \in \text{Homeo}_+(S^1) \mid g(x) = x, \forall x \notin X_1\} \cong \text{Homeo}_+(X_1)$ (we still call H_0 this subgroup of $\text{Homeo}_+(S^1)$). We now consider the subgroup $\langle H_0^t \mid t \in T \rangle$ obtained by spreading H_0 on the circle through conjugation by elements of T . Since $\text{supp}(H_0^t) \subseteq t(X_1)$ for any $t \in T$, the groups H_0^t have disjoint support hence they commute elementwise pairwise and $\langle H_0^t \mid t \in T \rangle \cong \prod_{t \in T} H_0^t$. Moreover, the conjugation action of T on $\langle H_0^t \mid t \in T \rangle$ permutes the subgroups H_0^t . It follows that

$$\langle H_0^t, T \mid t \in T \rangle = H_0 \wr T \hookrightarrow \text{Homeo}_+(S^1).$$

In case $T = \{t_1, \dots, t_k\}$ is finite, then it is a closed subset of S^1 . We define $X_i := (t_i, t_{i+1})$, for $i = 1, \dots, k$, where $t_{k+1} := t_1$. We can copy the same procedure of the infinite case, by noticing that $S^1 = \bigcup_{i=1}^k X_i \cup T$ and embedding H_0 into subgroups of $\text{Homeo}_+(S^1)$ isomorphic with $\text{Homeo}_+(X_i)$. \square

We now follow the previous proof, but we need to be more careful in order to embed Thompson's group $T = \text{PL}_2(S^1)$ into $\text{PL}_+(S^1)$.

Theorem 6.4.6. *There is an embedding $\varphi : \mathbb{Q}/\mathbb{Z} \hookrightarrow \text{PL}_2(S^1)$ such that $\text{rot}(\varphi(x)) = x$ for every $x \in \mathbb{Q}/\mathbb{Z}$ and there is an interval $I \subseteq S^1$ with dyadic endpoints such that $\varphi(x)I$ and $\varphi(y)I$ are disjoint, for all $x, y \in \mathbb{Q}/\mathbb{Z}$ with $x \neq y$.*

Proof. We consider the set of elements $\{x_n = 1/n! \mid n \in \mathbb{N}\}$ of \mathbb{Q} which are the primitive $n!$ -th roots of 1 in \mathbb{Q} with respect to the sum. Thus $nx_n = x_{n-1}$ for each n . We want to send each x_n to a homeomorphism X_n of $\text{PL}_2(S^1)$ with $\text{rot}(X_n) = 1/n!$ and such that $(X_n)^{n!} = \text{id}_{S^1}$ and so, since $\langle x_n \mid n \in \mathbb{N} \rangle = \mathbb{Q}/\mathbb{Z}$, we will have an embedding $\mathbb{Q}/\mathbb{Z} \hookrightarrow \text{PL}_2(S^1)$. For every positive integer n we choose and fix a partition P_n of the unit interval $[0, 1]$ into $2n - 1$ intervals whose length is a power of 2. To set up a notation, we always assume to look at S^1 from the origin

of the axes: from this point of view right will mean clockwise and left will mean counterclockwise and we will always read intervals clockwise.

If we have a partition of S^1 in $2m$ intervals, we define a “shift by 2” in $\text{PL}_2(S^1)$ to be the homeomorphism X which permutes the intervals of the partition cyclically and such that $\text{rot}(X) = 1/m$ and $X^m = \text{id}$. In other words, the “shift by 2” sends linearly an interval V to another interval W which is 2 intervals to the right of V .

We want to build a sequence of maps $\{X_n\}$ that acts on a partition of S^1 made by $2(n!)$ intervals $J_{n,1}, I_{n,1}, \dots, J_{n,n!}, I_{n,n!}$, that are ordered so that each one is on the right of the previous one. The map X_n acts as the “shift by 2” map on this partition. We define $X_1 = \text{id}$. To build X_2 , we cut S^1 in four intervals $I_{2,1}, J_{2,1}, I_{2,2}, J_{2,2}$ of length $1/4$, each one on the right of the previous one: X_2 is then defined to be the map which shifts linearly all these intervals by 2, thus sending the I 's onto the J 's and the J 's onto the I 's. X_2 is thus the rotation map by π . Assume now we have built X_n and we want to build X_{n+1} . We take the $2(n!)$ intervals of the partition associated to X_n and we divide each of the intervals $I_{n,i}$ according to the proportions given by the partition P_n , and thus cutting each $I_{n,i}$ into $2n+1 = 2(n+1)-1$ intervals. On the other hand, we leave all the $J_{n,i}$'s undivided. Now we have a partition of S^1 into

$$n! + (2n+1)n! = 2[(n+1)!]$$

intervals with dyadic endpoints. Starting $J_{n+1,i} := J_{n,i}$ we relabel all the intervals of the new partition by I 's and J 's. By shifting all the intervals by 2, we have defined a new piecewise linear map $X_{n+1} \in \text{PL}_2(S^1)$ (see figure 6.9 to see the construction of maps X_2 and X_3).

We need to verify that $(X_{n+1})^{n+1} = X_n$. We observe that $Y_n := (X_{n+1})^{n+1} \in \text{PL}_2(S^1)$

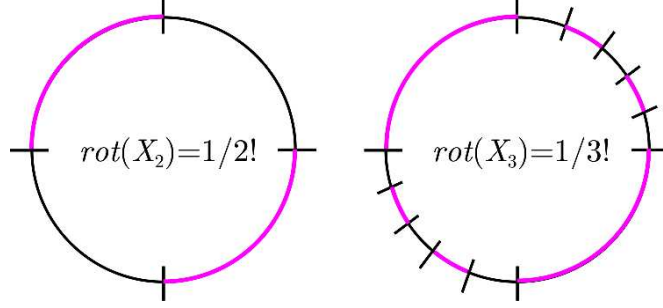


Figure 6.9: How to build the map X_3 from X_2 .

shifts every interval linearly by $2n+2$. By construction Y_n sends $J_{n,i}$ linearly onto $J_{n,i+1}$, while it sends $J_{n,i}$ piecewise-linearly onto $J_{n,i+1}$. All the possible break-points of Y_n on the interval $I_{n,i}$ occur at the points of the partition P_n , but it is a straightforward computation to verify that the left and right slope coincide at these points, thus giving that Y_n sends $J_{n,i}$ linearly onto $J_{n,i+1}$. To build the embedding $\varphi : \mathbb{Q}/\mathbb{Z} \rightarrow \text{PL}_2(S^1)$ we define $\varphi(x_n) := X_n$ and then extend it to a group homomorphism recalling that $\mathbb{Q}/\mathbb{Z} = \langle x_n \rangle$. The map φ must be injective since if $\varphi(x) = \text{id}$ then, by using the fact that $(X_{r+1})^{r+1} = X_r$ for any integer r , we can write $\text{id} = \varphi(x) = X_n^k$ for some suitable integers n, k , hence k is a multiple of $n!$ and we can rewrite x as $kx_n = (n!)x_n = 0$. Finally, we notice that for every $x, y \in \mathbb{Q}/\mathbb{Z}$, $x \neq y$ we have that $\varphi(x)(J_{2,1})$ and $\varphi(y)(J_{2,1})$ are disjoint. In fact, if we define $V = \varphi(y)(J_{2,1})$, then the two intervals can be rewritten as $\varphi(xy^{-1})(V)$ and V , and so, since φ is an embedding and $xy^{-1} \neq 1$, they must be distinct. \square

As an immediate consequence of the previous theorem, we get the following result.

Theorem 6.4.7. *For every $H \leq \mathbb{Q}/\mathbb{Z}$ there is an embedding $F \wr H \hookrightarrow T$, where F and T are the respective Thompson's groups and the wreath product $F \wr H = \left(\bigoplus F\right) \rtimes H$ is restricted.*

Proof. We prove it for the full group $H = \mathbb{Q}/\mathbb{Z}$. We apply the previous Theorem to build an embedding $\varphi : \mathbb{Q}/\mathbb{Z} \hookrightarrow \text{PL}_2(S^1)$. Moreover, by construction, the image $\varphi(\mathbb{Q}/\mathbb{Z})$ acts as permutations on the intervals $J_{n,i}$. Hence, we recover that

$$\text{PL}_2(J_{2,1}) \wr \mathbb{Q}/\mathbb{Z} \hookrightarrow \text{PL}_2(S^1). \quad \square$$

Theorem 6.4.8. *For every $H \leq \mathbb{Q}/\mathbb{Z}$ there is an embedding $\text{PL}_+(I) \wr H \hookrightarrow \text{PL}_+(S^1)$, where the wreath product $\text{PL}_+(I) \wr H = \left(\bigoplus \text{PL}_+(I) \right) \rtimes H$ is restricted.*

Proof. The proof of this result is similar to the one of Theorem 6.4.7, except that here we do not require the endpoints of the interval I to be dyadic. \square

Remark 6.4.9. We remark that none of the embedding results require the groups to have no non-abelian free subgroups. For Theorems 6.4.7 and 6.4.8 the absence of non-abelian free subgroups is guaranteed by the Brin-Squier Theorem [18]. However, we observe that in Theorem 6.4.5 we can have non-abelian free subgroups and still build the embedding.

6.5 Fixed-Point Free Actions on the Circle

Sacksteder's Theorem states that every fixed-point free action on the real line must be abelian (see Theorem 2.3 in [29]). The same result is true also for $G \leq \text{Homeo}_+(I)$ (see Lemma 4.4 by Plante-Thurston in [51]). Both Sacksteder's Theorem and Plante-Thurston's Lemma are proved by observing that G is an archimedean group and so they appeal to a Theorem of Holder (for a proof, see [29]). The following is an alternative proof of the well known version of Sacksteder's Theorem for subgroups of the group $\text{Homeo}_+(S^1)$.

Lemma 6.5.1. *Let $G \leq \text{Homeo}_+(S^1)$. Suppose that every element of $G \setminus \{id\}$ has no fixed points. If $f, g \in G$ are such that $\text{rot}(f) = \text{rot}(g)$, then $f = g$. Moreover, for every $h, k \in G$, we have that $[h, k] = id$.*

Proof. If $\text{rot}(f) = \text{rot}(g) \notin \mathbb{Q}/\mathbb{Z}$ then it has already been proved in Lemma 6.2.10(ii). We suppose now that $\text{rot}(f) = \text{rot}(g) = k/m \in \mathbb{Q}/\mathbb{Z}$, hence f^m, g^m both have fixed points. By definition of G this implies that $f^m = g^m = id_{S^1}$ and so $\widehat{f^m}(t) = \widehat{g^m}(t) + u$ for some integer u and for all $t \in \mathbb{R}$. We argue, by contradiction, that $f g^{-1}$ has no fixed points in S^1 . Thus we can assume $\widehat{f} > \widehat{g}$ on \mathbb{R} . If $u = 0$, then $\widehat{g^m}(t) < \widehat{f^m}(t) = \widehat{g^m}(t)$, which is a contradiction. If $u \neq 0$ then, for every positive integer r , we have

$$\begin{aligned} \widehat{f^{mr}}(t) &= \widehat{f^{m(r-1)}}(\widehat{f^m}(t)) = \widehat{f^{m(r-1)}}(\widehat{g^m}(t) + u) = \\ &= \widehat{f^{m(r-1)}}(\widehat{g^m}(t)) + u = \widehat{f^{m(r-2)}}(\widehat{g^m}(t) + u) + u = \\ &= \widehat{f^{m(r-2)}}(\widehat{g^m}(t)) + 2u = \dots = \widehat{g^{mr}}(t) + ur. \end{aligned}$$

Up to moving ur on the other hand side of the equation, we can assume $u > 0$ and divide by mr

$$\frac{\widehat{f^{mr}}(t)}{mr} = \frac{\widehat{g^{mr}}(t)}{mr} + \frac{u}{m}.$$

We send $r \rightarrow +\infty$ and we get

$$\text{rot}(f) = \text{rot}(g) + \frac{u}{m} > \text{rot}(g) = \text{rot}(f)$$

yielding a contradiction. For the second part, we just note that $\text{rot}(h) = \text{rot}(h^k)$.

□

Corollary 6.5.2. *Let $G \leq \text{Homeo}_+(S^1)$. Suppose that every element of $G \setminus \{id\}$ has no fixed points. Then G is abelian.*

CHAPTER 7

CENTRALIZERS OF SUBGROUPS OF $\text{HOMEO}_+(S^1)$

In this Chapter we give a description of centralizers of elements in $\text{PL}_+(S^1)$ and Thompson's group T . This analysis is a first step toward a possible solution of the simultaneous conjugacy problem. We recall that, if $G \leq \text{Homeo}_+(S^1)$, the subset of elements of G with a fixed point does not necessarily form a subgroup. In Chapter 6 we showed that this happens when G satisfies some additional requirements. In this Chapter we show that this is still the case when the group G is the centralizer in $\text{PL}_+(S^1)$ of elements in $\text{PL}_+(S^1)$ with rational rotation number. In certain cases, we can embed the subgroup of elements with fixed points in $\text{PL}_+(I)$ and use the results of Chapter 4 to describe it and write G as an extension of this subgroup. We will identify S^1 with \mathbb{R}/\mathbb{Z} to have a well defined origin 0 on S^1 . The material of this Chapter represents joint work with Collin Bleak and Martin Kassabov.

7.1 Centralizers of torsion elements

In this section we determine centralizers for torsion elements in $\text{Homeo}_+(S^1)$, in $\text{PL}_+(S^1)$ and Thompson's group T . In all of these cases, the strategy will be to conjugate the element to a rotation.

Convention 7.1.1. Let G be either of the symbols Homeo_+ or PL_+ or PL_2 . To make the treatment unified in this subsection, we will write $G(I), G(S^1), G(\mathbb{R})$ to refer to the groups $\text{Homeo}_+(I), \text{Homeo}_+(S^1), \text{Homeo}_+(\mathbb{R})$ (respectively $\text{PL}_+(I), \text{PL}_+(S^1), \text{PL}_+(\mathbb{R})$) and $\text{PL}_2(I), \text{PL}_2(S^1), \text{PL}_2(\mathbb{R})$.

Lemma 7.1.2. *Let G be either of the symbols Homeo_+ or PL_+ . Every torsion element of $G(S^1)$ is conjugate to a rotation.*

Proof. Let $f \in G(S^1)$ be such that $\text{rot}(f) = m/k$ and $f^k = \text{id} \in G(S^1)$. Since $(m, k) = 1$ are coprime there exist two integers α, β such that $\alpha m + \beta k = 1$ and so

$$\frac{1}{k} = \alpha \frac{m}{k} + \beta.$$

If we define $g = f^\alpha$, we have that $\text{rot}(g) = \text{rot}(f^\alpha) = \alpha \cdot \text{rot}(f) = \alpha \frac{m}{k} = \frac{1}{k} \pmod{1}$. Since $\text{rot}(g) = \frac{1}{k}$, we have $\widehat{g^k}(t) = t + 1$ by Lemma 6.1.2(iv) and the order of g is k so that $\langle f \rangle = \langle g \rangle$. We want to find $h \in G(\mathbb{R})$ such that $h(t + 1) = h(t) + 1$ and $\widehat{g}h(t) = h(t + \frac{1}{k})$, that is, a map h such that $h^{-1}\widehat{g}h$ is the translation by $\frac{1}{k}$.

Choose a real number $A \in [0, 1)$ and choose an orientation-preserving piecewise linear homeomorphism that sends the interval $[0, \frac{1}{k}]$ to the interval $[A, \widehat{g}(A)]$, hence $h(0) = A$ and $h(\frac{1}{k}) = \widehat{g}(A)$. We extend h to an element of $G(\mathbb{R})$ by defining

$$h(t) = \widehat{g^r}h\left(t - \frac{r}{k}\right)$$

if $t \in \left[\frac{r}{k}, \frac{r+1}{k}\right]$, for some integer r . By construction, we have that $\widehat{g}h(t) = h(t + \frac{1}{k})$ for all $t \in \mathbb{R}$. Hence, for any $t \in \mathbb{R}$, we have

$$h(t + 1) = h\left(t + k \frac{1}{k}\right) = \widehat{g^k}h(t) = h(t) + 1.$$

If we define $v \in G(S^1)$ as $v(t) := h(t) \pmod{1}$ we have that $\widehat{v} = h$ and v is a conjugator between g and a pure rotation $T_{\frac{1}{k}}$ by $\frac{1}{k}$. \square

Theorem 7.1.3. *Let G be either of the symbols Homeo_+ or PL_+ . Let $f \in G(S^1)$ be a torsion element. Then there exist two subgroups $H, K \leq C_{G(S^1)}(f)$ such that $H \cong G(I)$, $K \cong \mathbb{R}/\mathbb{Z}$ and $H \cap K = 1$, $C_{G(S^1)}(f) = HK$ and neither H nor K is a normal subgroup.*

Proof. By the previous result, there is an element $h \in G(S^1)$ such that $h^{-1}fh = T_\alpha$ rotation by $\alpha = \frac{m}{k}$. Up to taking a suitable power of f , we can assume that $m = 1$. Thus $C_{G(S^1)}(f) = C_{G(S^1)}(hT_\alpha h^{-1}) = hC_{G(S^1)}(T_\alpha)h^{-1}$. We want to find $C_{G(S^1)}(T_\alpha)$. We observe that $C_{G(S^1)}(T_\alpha)$ acts transitively on S^1 , since it contains the set H of all rotations of S^1 . By the previous result, we have that $K := \text{Stab}_{C_{G(S^1)}(T_\alpha)}(0) \cong G([0, \frac{1}{k}])$. Elements of K appear as follows: choose an element of $G([0, \frac{1}{k}])$ and copy it on each interval $[\frac{r}{k}, \frac{r+1}{k}]$, for $r = 0, \dots, k-1$. For any $g \in C_{G(S^1)}(T_\alpha)$, there is a rotation T_β such that gT_β fixes 0, and so $gT_\beta \in K$. Hence $H \cdot K = C_{G(S^1)}(T_\alpha)$ and, by construction, we have $H \cap K = 1$. It is easily seen that neither H nor K is normal in $C_{G(S^1)}(T_\alpha)$. \square

Remark 7.1.4. The product in the previous Lemma is a special instance of the Zappa-Szep product. An overview of this type of product can be found in [16]. We recall that a group G is the *Zappa-Szep product* of two subgroups H, K if $H \cap K = 1$, $HK = G$ but they are not necessarily normal in G .

There is another way to classify the centralizers of the previous Theorem. We are now going to give a description that will give information about centralizers in Thompson's group T too. The idea is similar to the one of Lemma 7.1.2: instead of conjugating the element to a rotation, we will rescale the circle to get an isomorphic group where the torsion element is indeed a rotation.

Theorem 7.1.5. *Let G be either of the symbols Homeo_+ or PL_+ or PL_2 . Let $g \in G(S^1)$ with $\text{rot}(g) = p/q \in \mathbb{Q}/\mathbb{Z}$, with p, q coprime numbers, and such that $g^q = \text{id}_{S^1}$. Then $C_{G(S^1)}(g)$ is a central extension*

$$1 \rightarrow C_q \rightarrow C_{G(S^1)}(g) \rightarrow G(S^1) \rightarrow 1$$

where C_q is the cyclic group of order q .

Proof. Since p and q are coprime numbers then, up to taking a suitable power, we can assume that $g \in G(S^1)$ with $\text{rot}(g) = 1/q$. In the case of $G(S^1) = T$, since 0 is dyadic then $g(0)$ is dyadic too. We choose $D := [0, g(0)]$ as a fundamental domain for the action of g , since

$$S^1 = \bigcup_{i=0}^{q-1} g^i(D) \quad \text{and} \quad g|_{g^i(D)} = g^i(g|_D).$$

We are now going to stretch the unit circle to a circle of “length q ”, by transforming the fundamental domain into an interval of length 1 and then reproducing g in this new setting. If this stretching is done carefully, using conjugation by a suitable map, the map g becomes a rotation, which is then simpler to centralize.

We look for a homeomorphism $H : \mathbb{R} \rightarrow \mathbb{R}$ such that

- $H(g^k(0)) = k$, for any integer k , and
- $H(g(x)) = t(H(x)) = H(x) + 1$, where $t(x) = x + 1$.

To construct H , choose any piecewise-linear homeomorphism $H : [0, g(0)] \rightarrow [0, 1]$ with finitely many breakpoints: it is immediate to find one such map in the cases $G = \text{Homeo}_+$ or $G = \text{PL}_+$. For the case $G = \text{PL}_2$ we apply theorem 1.1.5 to find a piecewise-linear homeomorphism with the additional requirement of having dyadic rational breakpoints and all slopes that are power of 2. Then we extend it to a map $H \in G(\mathbb{R})$ by defining

$$H(x) := H(g^{-k}(x)) + k \quad \text{if } x \in [g^k(0), g^{k+1}(0)] \text{ for some integer } k.$$

It is immediate to see, from the definition of H , that $H(g(x)) = t(H(x))$ for any real number x . By passing to quotients in $S_1^1 := [0, 1]/\{0, 1\}$ and $S_q^1 := [0, q]/\{0, q\}$, we get a map $h : S_1^1 \rightarrow S_q^1$, defined by $h(x \pmod{1}) := H(x) \pmod{q}$. Define a map

$$\begin{aligned} \varphi : G(S_1^1) &\mapsto G(S_q^1) \\ f &\mapsto hfh^{-1}. \end{aligned}$$

This map is clearly an isomorphism. By construction we have that $\varphi(g)$ is the rotation map $r : S_q^1 \rightarrow S_q^1$ defined by $r(x \pmod q) = t(x \pmod q) = x + 1 \pmod q$. We define two isomorphic copies of the group $G(S^1)$ by putting $G_1 := C_{G(\mathbb{R})}(t)/\langle t \rangle \cong G(S_1^1)$ and $G_2 := C_{G(\mathbb{R})}(t^q)/\langle t^q \rangle \cong G(S_q^1)$. Using the isomorphism φ it follows $C_{G_1}(g) \cong C_{G_2}(r)$, so we can study the second centralizer, as the rotation map r is easier to deal with.

Inside the circle S_q^1 the map r has rotation number $\text{rot}(r) = 1/q$. To compute the centralizer $C_{G_2}(r)$, we need to find all $v \in G_2$ that are induced by some map $V \in G(\mathbb{R})$ satisfying $V(x + q) = V(x) + q$ (since v is a map on the circle S_q^1) as well as the equality $V(x + 1) = V(x) + 1$ (since v centralizes the rotation r). In other words,

$$C_{G_2}(r) \cong \{V \in G(\mathbb{R}) \mid V(x + 1) = V(x) + 1\} / \langle t^q \rangle$$

By construction $\langle r \rangle$ is contained in the center of $C_{G_2}(r)$ and has order q . To conclude we just observe that the quotient is

$$\frac{C_{G_2}(r)}{\langle r \rangle} \cong \{V \in G(\mathbb{R}) \mid V(x + 1) = V(x)\} \cong G(S^1). \quad \square$$

Remark 7.1.6. We observe that the extension of Theorem 7.1.5 does not split. If the extension did split, following the proof of the Theorem, we would be able to write $C_{G_2}(r)$ as the direct product $\langle r \rangle \times G(S^1)$ where the element (r, id) has no q -th root. In fact, for any element $(x, y) \in \langle r \rangle \times G(S^1)$, we have $(x, y)^q = (id, y^q)$. However, we observe that the group $C_{G_2}(r)$ contains every rotation contained in G_2 . Hence it is possible to build a suitable rotation v in G_2 with rotation number $\frac{1}{q^2}$ such that $v^q = r$, leading to a contradiction.

7.2 Non-torsion elements with rational *rot* number

We can use the procedure of Theorem 7.1.5 and adapt it to the case of non-torsion elements. That is, we can stretch the fundamental domain of the action to become an interval of length 1 and then centralizers will be determined by their behavior on the fundamental domain. We begin with an elementary result that we will use in the rest of the sections of this chapter.

Lemma 7.2.1. *Let $G \leq \text{Homeo}(S^1)$ stabilizing a finite subset $X \subseteq S^1$. Then*

1. *If $g \in G$ fixes a point $x \in X$, then $g|_X = \text{id}_X$.*
2. *The restriction $G|_X$ is a cyclic group C_k , where k divides the size $|X|$.*
3. *Let $G_0 = \{g \in G \mid \text{rot}(g) = 0\}$. Then G_0 is a normal subgroup of G and $G/G_0 \cong \text{rot}(G) \cong C_k$.*

Proof. We order the points of X on the circle and label them as $\{1, 2, \dots, n\}$. Assume that $1 < g(1) = r \leq n$. We want to prove that g shifts all the elements of X by r units in the same direction. The map g sends the interval $[1, 2]$ into the interval $[r, g(2)]$. Since the map g is order preserving, we must have $g(2) > g(1)$ and $g(2) = r + 1$. Otherwise, if $g(2) > r + 1$, then we would have $1 < g^{-1}(r + 1) < 2$ and $g^{-1}(r + 1) \in X$. Similarly we prove that $g(i) = r + i - 1 \pmod{n}$. Hence $g = h^{r-1}$, where h is the map $h(i) = i + 1 \pmod{n}$. This is true for any $g|_X \in G|_X$, therefore $G|_X \leq \langle h \rangle$ and $G|_X$ is cyclic of order k , for some integer k . If v is the generator of $G|_X$, all of its orbits have size k and so, by the class equation, we have $|X| = km$, for some integer m . It also follows that if $g \in G$ fixes a point $x \in X$, then $g|_X = \text{id}_X$. Moreover, it is now immediate to see that if $g(1) = r$, then $\text{rot}(g) = r/n$ and so $\text{rot}(G) \cong C_k$.

Let now $g \in G_0$ and we can assume $0 \in \text{Fix}(g)$. Write $g \in \text{Homeo}_+([a, b])$ for some suitable interval $[a, b]$ of length 1. Since X is g -invariant and g preserves the orientation, then $g(i) = i$. Otherwise, $g(i) > i$ for all i and g is a shift map. But this would imply that $n < g(n) < b$ and $g(n) \in X$ and this is impossible, because X has only n elements. Hence G_0 must be precisely the kernel of the action of G . We conclude that $G/G_0 \cong G|_X$ and we are done. \square

Note 7.2.2. For the remainder of this Chapter, if H is a subgroup of $G(S^1)$, we denote by H_0 the subset of elements of H that have fixed points.

Lemma 7.2.3. *Let G be either of the symbols PL_+ or PL_2 . Let $g \in G(S^1)$ with $\text{rot}(g) = p/q \in \mathbb{Q}/\mathbb{Z}$ and such that $g^q \neq \text{id}_{S^1}$. Then $C_{G(S^1)}(g)_0$ is a subgroup and the group $C_{G(S^1)}(g)$ is an extension*

$$1 \rightarrow C_{G(S^1)}(g)_0 \rightarrow C_{G(S^1)}(g) \rightarrow C_k \rightarrow 1$$

where C_k is the cyclic group of order k .

Proof. Since the map g^q has fixed points, it can be considered as an element of $\text{PL}_+(J)$ for some interval J , hence the set $X := \partial \text{Fix}(g^q)$ is finite. The conclusion follows via Lemma 7.2.1, since $C_{G(S^1)}(g)$ stabilizes X . \square

Remark 7.2.4. The previous proof does not extend immediately to the case $\text{Homeo}_+(S^1)$ since the set $\partial \text{Fix}(g^q)$ is not always finite.

Theorem 7.2.5. *Let G be either of the symbols PL_+ or PL_2 . Let $g \in G(S^1)$ with $\text{rot}(g) = p/q \in \mathbb{Q}/\mathbb{Z}$ and such that $g^q \neq \text{id}_{S^1}$. Then $C_{G(S^1)}(g)$ is an extension*

$$1 \rightarrow G(I)^r \times \mathbb{Z}^s \rightarrow C_{G(S^1)}(g) \rightarrow C_k \rightarrow 1$$

where C_k is the cyclic group of order k .

Proof. By Lemma 7.2.3 it is sufficient to give a description of the subgroup $C_{G(S^1)}(g)_0$. We consider again the action of $\langle g \rangle$ acts on the finite set $X := \partial \text{Fix}(g^q)$. We choose a fundamental domain for the action of $\langle g \rangle$ on S^1 , that is an interval D such that $S^1 = \bigcup_{v=0}^{q-1} g^v(D)$. To do so we select inequivalent elements of X as endpoints of the intervals in such a way that they build a unique interval D . By definition of D we can write

$$g^q|_{h(D)} \circ h = h \circ g^q|_D$$

for every $h \in \langle g \rangle$, and so the structure of bumps of g^q on $h(D)$ is the same as it has on D . In particular, $(C_T(g)_0)|_D$ and $(C_T(g)_0)|_{h(D)}$ must be isomorphic, for every element $h \in \langle g \rangle$. Moreover since every element $h \in (C_T(g)_0)|_D$ centralizes $g^q|_D$ we can use Theorem 4.4.20(ii) to determine centralizers. In the case $G = \text{PL}_2$ we have two cases: (i) if $X \cap \mathbb{Z} \left[\frac{1}{2} \right] \neq \emptyset$, then $g^q|_D$ can be seen as an element of $G(I)$ and, by Theorem 4.4.20(ii), we have $C_{G(S^1)}(g^q)_0|_D \cong \mathbb{Z}^m \times F^n$. (ii) If $X \cap \mathbb{Z} \left[\frac{1}{2} \right] = \emptyset$, then we can still see g^q as an element of some $G(J)$ for some interval J with non-dyadic endpoints and apply Theorem 4.4.20(ii) because the Stair Algorithm is valid independently of the endpoints. Hence, since no fixed point of g^q is dyadic the centralizer is generated by a suitable root of g^q and is thus infinite cyclic, i.e. $C_{G(S^1)}(g^q)_0|_D \cong \mathbb{Z}$. In the case $G = \text{PL}_+$, we only have case (i) and we get again that $C_{G(S^1)}(g^q)_0|_D \cong \mathbb{Z}^m \times \text{PL}_+(I)^n$. \square

7.3 More results on Centralizers

There are many more cases to be explored. We conclude with some results and a discussion leading to the more difficult and general cases, i.e. the presence of elements with irrational rotation number or the classification of centralizers of

subgroups.

Lemma 7.3.1. *Let $f \in \text{PL}_+(S^1)$ be such that $\text{rot}(f) \notin \mathbb{Q}/\mathbb{Z}$, then $C_{\text{PL}_+(S^1)}(f)$ can be embedded in \mathbb{R}/\mathbb{Z} .*

Proof. By Denjoy's Theorem 6.1.4, there is an $h \in \text{Homeo}_+(S^1)$ such that $h^{-1}fh = T_\alpha$, the rotation by α . Then the map $\varphi(g) := hgh^{-1}$ sends $C_{\text{PL}_+(S^1)}(f)$ injectively into $C_{\text{Homeo}_+(S^1)}(T_\alpha)$. It is a well known fact that $C_{\text{Homeo}_+(S^1)}(T_\alpha) \cong \mathbb{R}/\mathbb{Z}$. \square

The previous result is not a complete classification and it is left open for future work. We describe now some possible directions toward a complete classification. Suppose H is a subgroup of $\text{PL}_+(S^1)$. If H has no non-abelian free subgroups, we can use the fact that H can be described as an extension by Theorem 6.4.1 as a starting point for describing $C_{\text{PL}_+(S^1)}(H)$. However, if H has non-abelian free subgroups, the structure of centralizers can partially be described. Recall that if the set

$$\{h \in H \setminus \{id\} \mid \text{Fix}(h) \neq \emptyset\}$$

is empty then H must be abelian by Theorem 6.5.2. This could be again a starting point for describing $C_{\text{PL}_+(S^1)}(H)$. If some element of H has a fixed point, we have the following result.

Theorem 7.3.2. *Let $H \leq \text{PL}_+(S^1)$. Assume that H has a non-abelian free subgroup and contains an element h_0 such that $\text{Fix}(h_0) \neq \emptyset$. Then $C_{\text{PL}_+(S^1)}(H) \cong C_k$, for some finite cyclic group C_k .*

Proof. Let $x_0 \in \partial \text{Fix}(h_0)$ and fix an orientation on the circle so that we can define intervals. The proof then divides naturally into several steps.

Claim 1. $X := \partial \text{Fix}(h_0)$ is a finite $C_{\text{PL}_+(S^1)}(H)$ -invariant subset of S^1 .

Proof. The first part follows from the fact that H commutes with h_0 . \square

Claim 2. H has no global fixed point.

Proof. Assume, by contradiction, that $y \in \text{Fix}(H)$, then we can fix y as an origin and write $H \leq \text{PL}_+(I)$. This is impossible because $\text{PL}_+(I)$ has no non-abelian free subgroups by the Brin-Squier Theorem [18]. \square

Claim 3. The set $C_{\text{PL}_+(S^1)}(H)$ is a normal subgroup and, for any $\gamma \in C_{\text{PL}_+(S^1)}(H)_0$, we have $\gamma|_X = \text{id}_X$.

This follows from Lemma 7.2.1(iii), because $C_{\text{PL}_+(S^1)}(H)_0$ is the kernel of the action of $C_{\text{PL}_+(S^1)}(H)$ on X . \square

Claim 4. The subgroup $C_{\text{PL}_+(S^1)}(H)_0$ is trivial.

Proof. Let now C be the largest connected set containing x_0 on which γ is the identity. Assume by contradiction that $C \neq S^1$, so that C is a suitable interval (a, b) . By Claim 2 $b \notin \text{Fix}(H)$, so there is an $h_1 \in H$ with an orbital (x_-, x_+) containing b , that is $x_-, x_+ \in \text{Fix}(h_1)$ and $(x_-, x_+) \subseteq S^1 \setminus \text{Fix}(h_1)$. Consider the restrictions $\bar{\gamma} := \gamma|_{(x_-, x_+)}$ and $\bar{h}_1 := h_1|_{(x_-, x_+)}$. Since $[\bar{\gamma}, \bar{h}_1] = \text{id}|_{(x_-, x_+)}$ and \bar{h}_1 is a one-bump function, Theorem 4.4.20(i) implies that $\bar{\gamma}$ is a power of some root of \bar{h}_1 and, in particular, $\bar{\gamma}$ is a one-bump function on (x_-, x_+) . The map $\bar{\gamma}$ fixes the midpoint of (x_-, b) , therefore $\bar{\gamma} = \text{id}|_{(x_-, x_+)}$, hence γ is the identity on (a, x_+) , contradicting the maximality of C . Therefore $C = S^1$ and, more generally, $K = \{\text{id}\}$. \square

The conclusion now follows via Lemma 7.2.1. \square

CHAPTER 8

A GROWTH FORMULA FOR THOMPSON'S GROUP F

In this final Chapter we provide an algorithm to compute the size of the balls in Thompson's group F with respect to the standard 2-element generating set. We briefly review the definition of "growth of a group". Let G be a finitely generated group with a fixed generating set S . For $n \in \mathbb{N}$, let B_n denote the ball of radius n in the Cayley graph of G . The *growth function* for G is defined as

$$\begin{aligned} \gamma : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto |B_n| \end{aligned}$$

Moreover, the *growth rate* of G is defined to be the limit

$$\lim_{n \rightarrow \infty} \sqrt[n]{|B_n|}.$$

Guba [36] and Burillo [23] give estimates for lower bounds of the growth rate. We recall that Thompson's group F has the following infinite presentation

$$\langle x_0, x_1, x_2, \dots \mid x_k^{-1} x_n x_k = x_{n+1}, \forall k < n \rangle$$

Since $x_k = x_0^{1-k} x_1 x_0^{k-1}$ for $k \geq 2$ the group F is generated by the elements x_0 and x_1 . We will use *forest diagrams* introduced by Belk and Brown in [4] to give a procedure to compute the size of the n -balls with respect to x_0 and x_1 , which may lead to information on the growth rate, or at least provide better bounds than those already known. We remark that it is an ongoing open question to determine the *growth series* of Thompson's group F (the generating function of the sequence

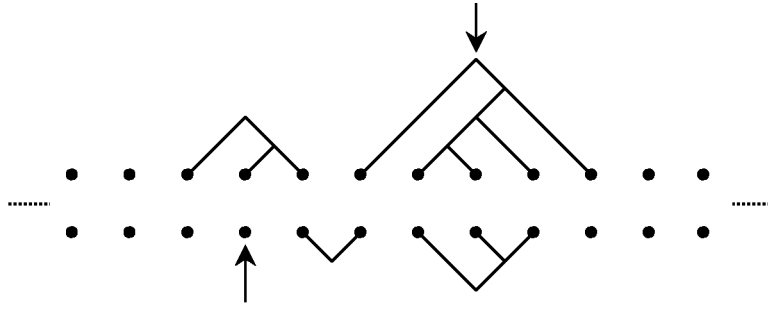


Figure 8.1: A forest diagram for an element of F .

$\{|B_n|\}_{n \in \mathbb{N}}$), or at least to detect whether or not it is rational or algebraic.

8.1 Forest Diagrams

The idea of this Chapter is to use forest diagrams introduced by Belk and Brown in [4] to find a recursion formula for a partition of the ball of radius n . We will use their length formula for forest diagrams to calculate distances in the Cayley graph of F . Let Γ denote the *Cayley graph* of F . This graph has a vertex for each element of F and an edge from f to xf for every $x \in \{x_0, x_1\}$. The *distance* between two points in the Cayley graph is the length of a minimal path between them. The *norm* $\ell(v)$ of a vertex $v \in \Gamma$ is the distance from v to the identity vertex of Γ . Each vertex of Γ can be represented by a *forest diagram* as shown in figure 1. Such a diagram consists of a pair of bounded, bi-infinite binary forests (*the top forest* and the *bottom forest*) together with an order-preserving bijection of their leaves. Let us be a bit more precise about these definitions. A *bi-infinite binary forest* is a sequence $(\dots, T_{-1}, T_0, T_1, \dots)$ of finite binary trees. We can represent such a forest as a line of trees, together with a pointer at the tree T_0 (as in figure 8.1).

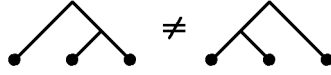


Figure 8.2: Different trees

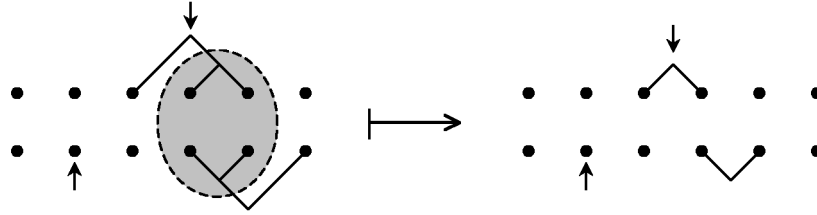


Figure 8.3: Reductions in a forest diagram.

A forest is *bounded* if only finitely many of its trees are nontrivial. Note that our binary trees are planar, i.e., the trees showed in figure 8.2 are different.

In particular, any binary tree comes with a linear ordering on its leaves; and this in turn induces a linear ordering on the leaves of a bi-infinite binary forest. A *caret* is a pair of edges in a forest that join two vertices to a common parent. We call a caret *grounded* if it joins two leaves. A *reduction* of a forest diagram consists of removing an opposing pair of grounded carets (see figure 8.3).

The inverse of a reduction is called an *expansion*. Two forest diagrams are *equivalent* if one can be transformed into the other by a sequence of reductions and expansions. A forest diagram is *reduced* if it does not have any opposing pairs of grounded carets. It turns out that every forest diagram is equivalent to a unique reduced forest diagram.

Proposition 8.1.1 ([4], Section 4). *There is a one-to-one correspondence between vertices of Γ and equivalence classes of forest diagrams. Therefore, every ele-*

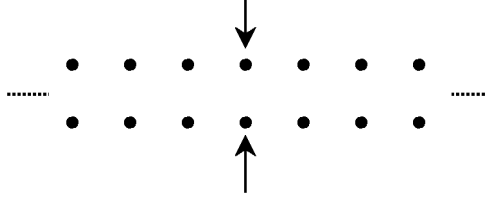


Figure 8.4: The trivial forest diagram.

ment of F can be represented uniquely by a reduced forest diagram.

Remark 8.1.2. We will frequently identify vertices of Γ , elements of F , and reduced forest diagrams. For example, if $f \in F$, we might talk about the “top forest of f ”. We hope this will not cause any confusion.

The forest diagram for the identity is showed in figure 8.4.

Given a forest diagram for a vertex $v \in \Gamma$, it is easy to find forest diagrams for the neighbors of v :

Proposition 8.1.3 ([4], Section 4). *Let \mathfrak{f} be a reduced forest diagram representing the vertex $v \in \Gamma$. Then:*

1. *A forest diagram for x_0v can be obtained by moving the top pointer of \mathfrak{f} one tree to the right.*
2. *A forest diagram for x_1v can be obtained by “dropping a caret at the current position”. That is, the forest diagram for x_1v can be obtained by attaching a caret to the roots of the top trees in \mathfrak{f} indexed by 0 and 1. Afterward, the top pointer points to the root of the new, combined tree.*

The bottom forest remains unchanged in either case. Note that the given forest diagram for x_1v will need to be reduced if the new caret opposes a grounded

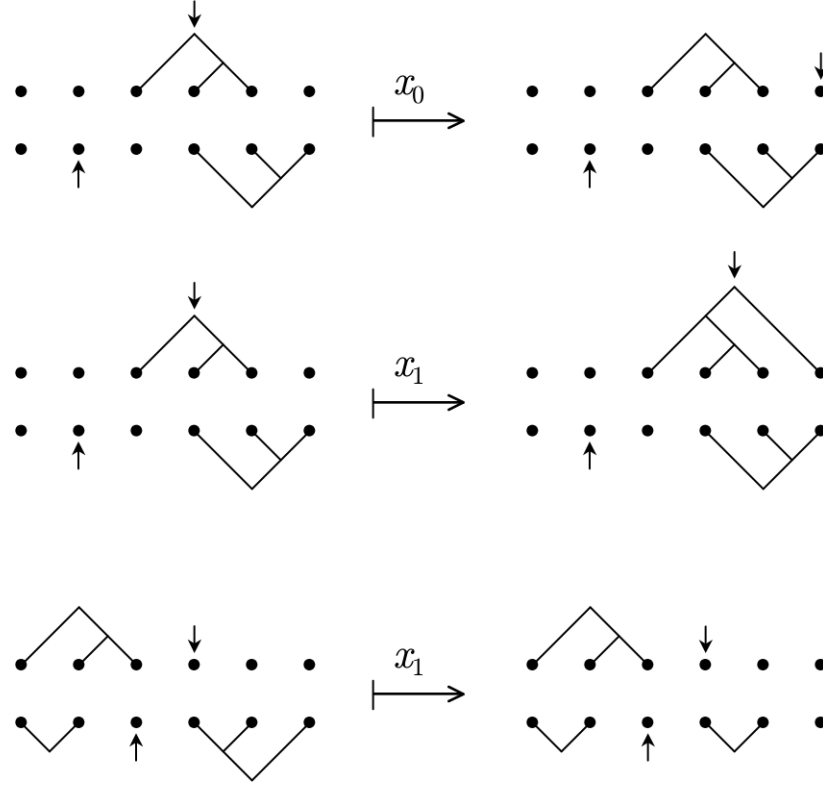


Figure 8.5: Some sample edges from the Cayley graph of F .

caret from the bottom tree. In this case, left-multiplication by x_1 effectively deletes a grounded caret from the bottom tree.

Corollary 8.1.4. *Again, let \mathfrak{f} be a reduced forest diagram for a vertex $v \in \Gamma$. Then:*

1. *A forest diagram for $x_0^{-1}v$ can be obtained by moving the top pointer of \mathfrak{f} one tree to the left.*
2. *A forest diagram for $x_1^{-1}v$ can be obtained by deleting the top caret of the current tree. The top pointer ends at the resulting left-child tree. If the current tree is trivial, one must first perform an expansion. In this case, left-multiplication by x_1^{-1} effectively creates a new grounded caret in the bottom tree.*

8.2 The Length Formula

Since the action of x_0 and x_1 is relatively simple, it comes as no surprise that one can find the length $\ell(f)$ of an element $f \in F$ directly from a forest diagram. Our treatment of the length formula is based on [4]. We begin with some terminology. A *space* is the region between two leaves in a forest. A space is *interior* if it lies between two leaves from the same tree, and *exterior* if it lies between two trees. Note that every exterior space in a forest is either to the left or the right of the pointer. Given a forest diagram for an element $f \in F$, we label the spaces between the leaves of each forest as follows. Label a space:

L (for left) if it is exterior and to the left of the corresponding pointer,

N (for necessary) if it is not of type **L** and if the leaf to the right of the space is a left leaf in its caret,

I (for interior) if it is interior and not of type **N**, or

R (for right) if it is exterior, to the right of the corresponding pointer, and not of type **N**. See figure 8.6 for an example. The spaces of a forest diagram come in pairs: one from the top forest and one from the bottom forest. The *support* of a forest diagram is the minimum interval that contains both pointers and all nontrivial trees. We only label space pairs in the support of a forest diagram. The *weight* of a space pair is determined by the table 8.1.

We can now state the length formula for elements of F . We follow the exposition in Section 5 of [4], which is a simplification of Fordham's original formula [30]. Viewing Thompson's group as a diagram group, Guba [36] has recently obtained a different version of the length formula.

	N	I	R	L
N	2	2	2	1
I	2	0	0	1
R	2	0	2	1
L	1	1	1	2

Table 8.1: The table of weight of the spaces

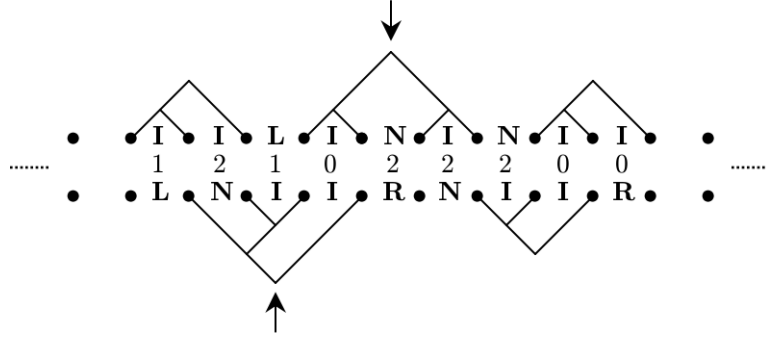


Figure 8.6: The length of this element is 22

Theorem 8.2.1 (Length Formula [4]). *Let $f \in F$, and let \mathfrak{f} be its reduced forest diagram. Let $\ell_1(f)$ be the total number of carets of \mathfrak{f} , and let $\ell_0(f)$ be the sum of the weights of all space pairs in the support of \mathfrak{f} . Then f has length*

$$\ell(f) = \ell_1(f) + \ell_0(f)$$

An element of F is called *positive* if it lies in the submonoid generated by $\{x_0, x_1, x_2, \dots\}$. Using the length formula, it is possible to estimate the growth of the elements of the positive monoid with respect to the $\{x_0, x_1\}$ generating set:

Theorem 8.2.2 (Belk-Brown [4]; Burillo [23]). *Let p_n denote the number of positive elements of length n , and let:*

$$p(x) = \sum_{n=0}^{\infty} p_n x^n$$

Then:

$$p(x) = \frac{1 - x^2}{1 - 2x - x^2 + x^3}$$

In particular, p_n satisfies the recurrence relation:

$$p_n = 2p_{n-1} + p_{n-2} - p_{n-3}$$

for large n .

Using a proof similar to that given by Belk-Brown in [4] we obtain a recurrence formula for a partition of the n -sphere of F , thus getting estimates for the growth rate.

8.3 Partitioning the n -sphere

We wish to cut the n -sphere so that there is a recurrence formula between the sizes of the slices. In order to do so, we need to establish some notations to define how to cut the ball of radius n . Throughout this section, \mathfrak{f} will be a reduced forest diagram for an element $f \neq x_0^k$ for all $k \in \mathbb{Z}$: this assumption will assure that there exists a nontrivial tree in the diagram \mathfrak{f} . By looking at the diagram \mathfrak{f} we define $(\begin{smallmatrix} t \\ s \end{smallmatrix})$ to be the rightmost pair of corresponding leaves of \mathfrak{f} such that at least one of the two leaves belongs to a non-trivial tree. Let T_+ be the tree of the top forest with t as its rightmost leaf and let T_- be the tree of the bottom forest with s as its rightmost leaf. We define the *critical space* $E = E(f)$ be the space to the right of the pair $(\begin{smallmatrix} t \\ s \end{smallmatrix})$ and we denote it by a vertical line passing through it (see figure 8.7).

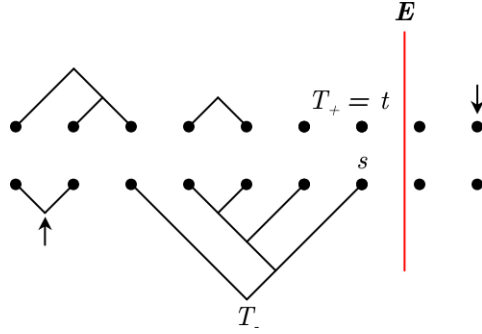


Figure 8.7: The trees T_+ , T_- and the line $E = E(f)$.

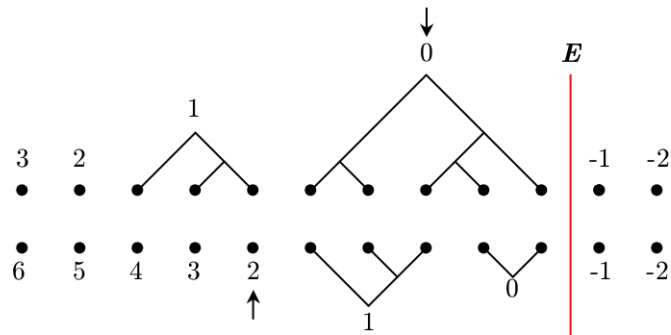


Figure 8.8: In this case $u(f) = 0$ and $w(f) = 5$.

8.3.1 Weights of the indicated trees

We order both the forests from right to left by placing an integer on each tree such that the two trees T_+, T_- correspond to the zeroes. Then we define (see figure 8.8):

$u(f)$ = index of the tree corresponding to the top pointer

$w(f)$ = index of the tree corresponding to the bottom pointer

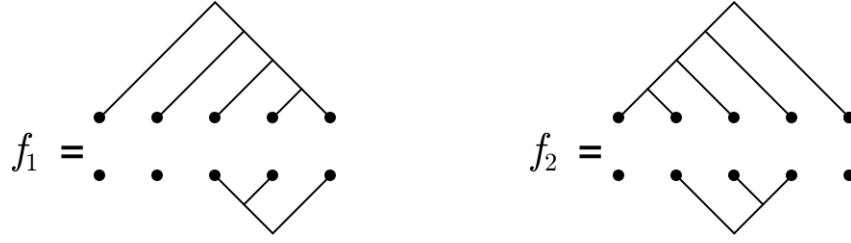


Figure 8.9: Here $b(f_1) = 4, c(f_1) = 1, b(f_2) = 1, c(f_2) = 0$.

8.3.2 Length of arcs of right edges

Given a binary tree T , whether it is oriented upward or downward, we define its *right arm* to be the longest path in T starting from the root and made only of right edges. Then define:

$$b(f) = \text{number of edges of the right arm of } T_+$$

$$c(f) = \text{number of edges of the right arm of } T_-$$

Notice that we always have $\max\{b(f), c(f)\} > 0$ (see figure 8.9).

8.3.3 Slices of the n -sphere

For $(i, j) \in \mathbb{N} \times \mathbb{N} \setminus \{(0, 0)\}$, $p, q \in \mathbb{Z}$ and $n \in \mathbb{N}$ we define the subsets

$$Z_{i,j,p,q,n} = \left\{ f \in F \setminus \langle x_0 \rangle \left| \begin{array}{l} b(f) = i, \quad c(f) = j, \\ u(f) = p, \quad w(f) = q, \\ \ell(f) = n \end{array} \right. \right\}.$$

For a fixed n , this family of sets forms a partition of the n -sphere. It is immediate that the inverses are related by

$$(Z_{i,j,p,q,n})^{-1} = Z_{j,i,q,p,n}$$

because inverting a forest diagram means turning it upside down. Thus we can always assume that $q \leq p$, that is “the bottom pointer is always on the right of the top pointer”. The interesting cases happen when we find $\max\{i, j, |p|, |q|\} \leq n$, in fact:

(a) If $i > n$, T_+ has more than n carets so by the length formula $\ell(f) > n$ and $Z_{i,j,p,q,n} = \emptyset$. Similarly the same is true for $j > n$.

(b) If $p > n$, there are more than n spaces of type (\mathbf{X}, \mathbf{Y}) with $\mathbf{X} = \mathbf{N}$ or $\mathbf{Y} = \mathbf{R}$. Moreover, a space of type (\mathbf{I}, \mathbf{R}) , must have a caret in the top forest. Each of the spaces in the support has weight ≥ 1 and so $\ell(f) > n$.

(c) If $q < -n$, there are more than n spaces of type (\mathbf{L}, \mathbf{Y}) , for any \mathbf{Y} and so their weight is at least 1 and so $\ell(f) > n$ again.

8.4 A recurrence formula for the slices in 5 variables

We define a map which shortens the length of elements and we will show how to keep track of this reduction. This will provide the desired relation.

8.4.1 The Shortening Map λ .

On each slice $Z_{i,j,p,q,n}$ we define a map λ , provided that p, q are positive integers, $i > 0$ for the map λ :

$$\begin{aligned} \lambda : Z_{i,j,p,q,n} &\longrightarrow F \\ f &\longmapsto x_{p+1}^{-1}f, \end{aligned}$$

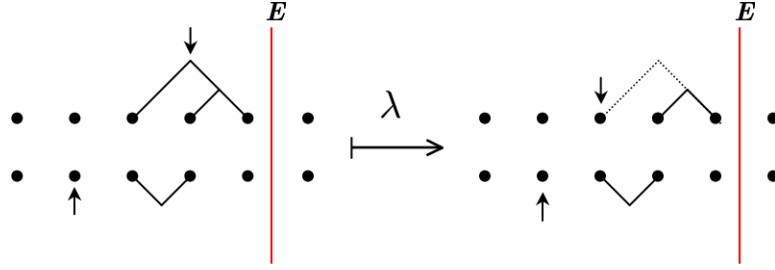


Figure 8.10: The action of λ when the top pointer is on T_+ .

where $x_{r+1} = x_0^{-r} x_1 x_0^r$. By construction, we see that $\lambda(f)$ is already reduced as a forest diagram and λ is an injective map. The map λ removes the top caret of the tree $T_+(f)$ and adjusts the top pointer in the following way:

- if the top pointer of \mathfrak{f} is not on $T_+(f)$, then we do not move it
- if the top pointer of \mathfrak{f} is on $T_+(f)$, then the top pointer of $\lambda(f)$ falls on the left of the two subtrees of $T_+(f)$ (see figure 8.10).

In other words, if $f \in Z_{i,j,p,q,n}$ then the p is the number of the tree where we must add a caret to get back f from $\lambda(f)$.

8.4.2 Length reduction of λ

Let (\mathbf{Y}, \mathbf{X}) the type of the space under the root of $T_+(f)$ and (\mathbf{V}, \mathbf{X}) the type of the space under the root of $T_+(\lambda(f))$. By definition of λ , the top pointer of $\lambda(f)$ is always on the left of the space (\mathbf{V}, \mathbf{X}) . We look at all the possibilities for the weights of the spaces (\mathbf{Y}, \mathbf{X}) and (\mathbf{V}, \mathbf{X}) (see figures 8.11 and table 8.2).

We notice that, if the type of space (\mathbf{Y}, \mathbf{X}) is different from (\mathbf{I}, \mathbf{R}) , then $\ell(\lambda(f)) = \ell(f) - 1$, because the map λ removes only a caret and it does not move the space

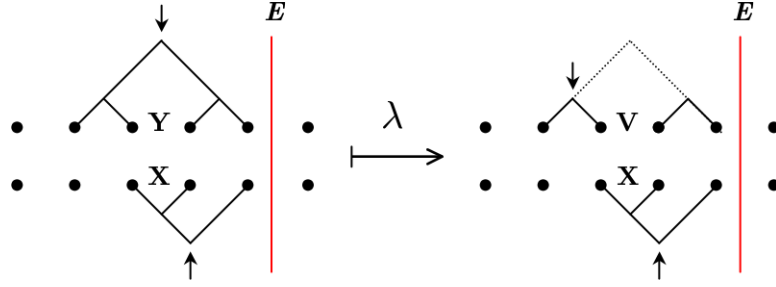


Figure 8.11: The various possibilities for (Y, X) and (V, X)

(Y, X)	weight	(V, X)	weight
(N, N)	2	(N, N)	2
(I, N)	2	(R, N)	2
(N, I)	2	(N, I)	2
(I, I)	0	(R, I)	0
(N, R)	2	(N, R)	2
(I, R)	0	(R, R)	2
(N, L)	1	(N, L)	1
(I, L)	1	(R, L)	1

Table 8.2: How λ reduces the length of elements

$E = E(f)$. In the case (Y, X) is of type (I, R) , then the space (V, X) is now of type (R, R) and it is out of the support of $\lambda(f)$ so we do not count it for the evaluation of length $\lambda(f)$, therefore $\ell(\lambda(f)) \leq \ell(f) - 1$ (see figure 8.12).

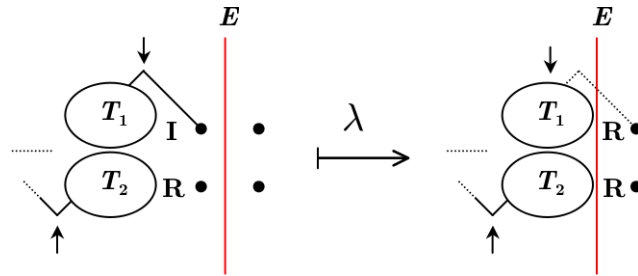


Figure 8.12: In each case $\ell(\lambda(f)) \leq \ell(f) - 1$.

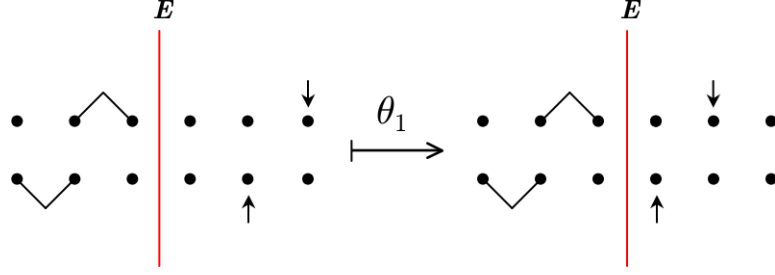


Figure 8.13: The map θ_1 .

8.4.3 The case $p < 0$

Define

$$\begin{aligned} \theta_1 : Z_{i,j,p,q,n} &\longrightarrow Z_{i,j,p+1,q+1,n-2} \\ f &\longmapsto x_0^{-1} f x_0 \end{aligned}$$

so that θ_1 moves both pointers by one space to the left. By construction θ_1 is bijective and $\ell(\theta_1(f)) = \ell(f) - 2$. In fact, either a space of type $(\mathbf{L}, \mathbf{L}) = 2$ is lost, or a space of type $(\mathbf{R}, \mathbf{L}) = 1$ is lost and one of type $(\mathbf{L}, \mathbf{L}) = 2$ becomes an $(\mathbf{R}, \mathbf{L}) = 1$. Therefore:

$$|Z_{i,j,p,q,n}| = |Z_{i,j,p+1,q+1,n-2}|$$

8.4.4 The case $q < 0 \leq p$

Define

$$\begin{aligned} \theta_2 : Z_{i,j,p,q,n} &\longrightarrow Z_{i,j,p,q+1,n-1} \\ f &\longmapsto f x_0 \end{aligned}$$

so that θ_2 moves the bottom pointer by one space to the left. This map is bijective and $\ell(\theta_2(f)) = \ell(f) - 1$, since only a space of type $(\mathbf{R}, \mathbf{L}) = 1$ is lost. Thus:

$$|Z_{i,j,p,q,n}| = |Z_{i,j,p,q+1,n-1}|$$

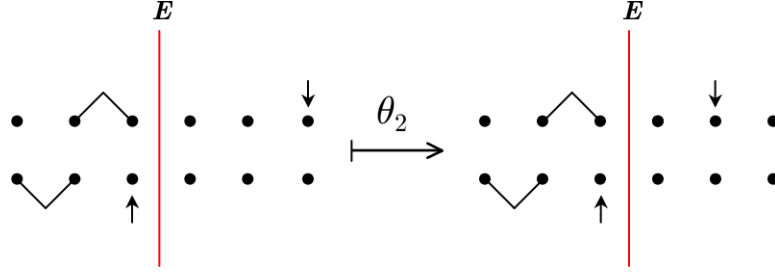


Figure 8.14: The map θ_2 .

8.4.5 The case $q \geq 0$ and $i + j \geq 2$

By definition of the shortening map λ it is easy to verify the following three equalities:

$$\lambda(Z_{i,j,p,q,n}) = Z_{i-1,j,p+1,q,n-1} \quad \forall i \geq 1, j \geq 1$$

$$\lambda((Z_{i,j,p,q,n})^{-1}) = (Z_{i,j-1,p,q+1,n-1})^{-1} \quad \forall i \geq 1, j \geq 1$$

$$\lambda(Z_{i,0,p,q,n}) = Z_{i-1,0,p+1,q,n-1} \quad \forall i \geq 2$$

8.4.6 The case $q = j = 0$ and $i = 1$

Using the map λ it can be seen that:

$$\lambda(Z_{1,0,p,0,n}) = \left(\bigcup_{\substack{c,d=0, \\ \max\{c,d\}>0}}^n \bigcup_{r=-n}^{-1} Z_{c,d,r+p+1,r,n-1} \right) \cup \{x_0^{1-n}\}$$

In fact, when we apply λ to an element of $f \in Z_{1,0,p,0,n}$ then $\lambda(f)$ can have no E -line, and so $\lambda(f) = x_0^{1-n}$ or it can still have an E -line, which is moved to the left by a suitable number of spaces. In this second case, what happens is that

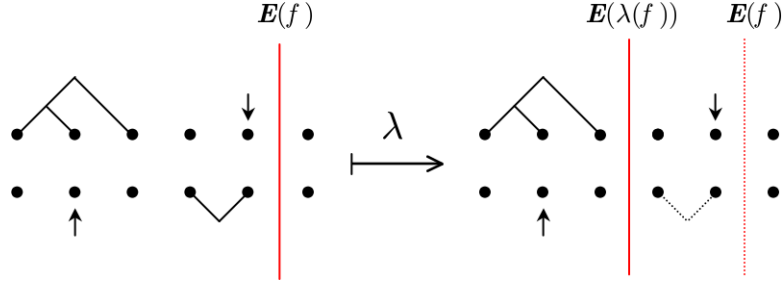


Figure 8.15: $\text{supp}(f) = \text{supp}(\lambda(f))$.

by applying the map λ we remove a top caret on the right, but since the bottom pointer of f was on the rightmost leaf inside $\text{supp}(f)$ then $\text{supp}(\lambda(f))$ still contains the same number of spaces, that is $\text{supp}(f) = \text{supp}(\lambda(f))$ (see figure 8.15).

8.4.7 The case $q > 0 = j$ and $i = 1$

The final case to observe by using the shortening maps is this:

$$\lambda(Z_{1,0,p,q,n}) = \left(\bigcup_{\substack{c,d=0, \\ \max\{c,d\}>0}}^n \bigcup_{r=0}^{q-1} Z_{c,d,r+p+1-q,r,n-2(r-(q-1))-1} \right) \cup \\ \cup \left(\bigcup_{\substack{c,d=0, \\ \max\{c,d\}>0}}^n \bigcup_{r=-n}^{-1} Z_{c,d,r+p+1-q,r,n-2(q-1)-1} \right) \cup \{x_0^{p+1-q}\}$$

In fact, when we apply λ to an element of $f \in Z_{1,0,p,q,n}$ then $\lambda(f)$ can have no E -line, and so $\lambda(f) = x_0^{p+1-q}$ or it can still have an E -line, which is moved to the left by a suitable number of spaces. In this second case, what happens is that by applying the map λ we remove a bottom caret on the right, but we have to

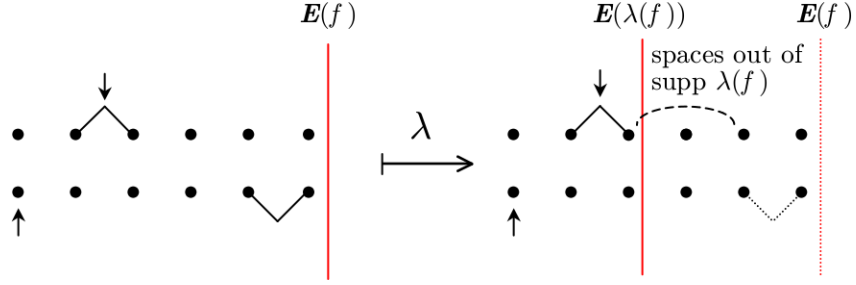


Figure 8.16: $\text{supp}(\lambda(f))$ may be reduced.

consider the fact that the support of $\lambda(f)$ is now reduced with respect from that of f . There might be empty spaces in f , between the rightmost caret and the first tree we find immediately to the left of it, and so we need to keep track of this in the union on the left. We need to consider all the possibilities for the position of the new E -line (see figure 8.16).

8.4.8 Commuting parameters

Define the following map

$$\begin{aligned} \varphi : Z_{1,0,p,q+1,n} &\longrightarrow Z_{1,0,q,p+1,n} \\ f &\longmapsto x_{q+1}f^{-1}x_{p+1} \end{aligned}$$

It is immediate that this is a bijection.

8.5 Reducing the recurrence to 3 variables

In this section we put together all the information about the slices and lower the number of parameters from 5 to 3. We will use the following notation: if

we write a sum $\sum_a^b(\dots)$ where $b < a$ then this sum symbol will denote zero. For example $\sum_{i=3}^2 i^2 = 0$. Now we define, for positive $p, q, n \in \mathbb{Z}$:

$$z(p, q, n) = |Z_{1,0,p,q+1,n}|.$$

Moreover we define $z(p, q, n) = 0$ for all negative $p, q, n \in \mathbb{Z}$. It is immediate from the definition and the bijection of Subsection 8.4.8 that

$$z(p, q, n) = z(q, p, n)$$

If we let $v = \min\{p, q\}$ and $s = \max\{p, q\}$, then we can decompose the n -ball in slices of the types described in the previous section. We start by applying the formula of Subsection 8.4.6 or Subsection 8.4.7. Then we apply the map λ to the remaining pieces and use the formulas of Subsections 8.4.3, 8.4.4 and 8.4.5 to remove carets and move the pointers in order to obtain a slice of the type $Z_{1,0,a,b+1,c}$. It is a straightforward computation to see that

$$\begin{aligned} z(p, q, n) = & \sum_{i,j=0}^n \sum_{r=0}^{v-1} z(p-r+i-1, q-r+j-1, n-2r-i-j) - \\ & + \sum_{r=0}^{v-1} z(p-r-1, q-r-1, n-2r) + \\ & + \sum_{\substack{i,j=0 \\ i \geq 1}}^n \sum_{\substack{r=v \\ s-1}}^{s-1} z(i-1, s-r+j-1, n-v-r-i-j) + \\ & + \sum_{j=1}^n \sum_{r=v}^{s-1} z(0, s-r+j, n-v-r-j-1) + \\ & + \sum_{i,j=1}^n \sum_{r=s}^{s+n} z(i-1, j-1, n-v+s-2r-i-j) + \\ & + \sum_{i=1}^n \sum_{r=s}^{s+n} z(i-1, 0, n-v+s-2r-i-j-1) + \\ & + \sum_{j=1}^n \sum_{r=s}^{s+n} z(0, j-1, n-v+s-2r-i-j-1) \end{aligned}$$

8.6 Open Question: the Growth Series of F

Let G be a finitely generated group with a fixed generating set S and let γ denote the associated growth function. We recall that the limit

$$\gamma := \lim_{n \rightarrow \infty} \sqrt[n]{\gamma(n)}$$

is called *growth rate* of G with respect to S . We say that G has *exponential growth* if this limit is positive. It can be shown that Thompson's group F has exponential growth with respect to the generating set $\{x_0, x_1\}$ (see [25]). Although, the precise growth rate is not known, some estimates have been given by Burillo [23], proving that γ cannot be less than the largest root of the equation $x^3 - x^2 - 2x + 1 = 0$, that is $\gamma \geq 2.2469796\dots$, and later were improved by Guba [36], showing that $\gamma \geq \frac{3+\sqrt{5}}{2}$. The *growth series* of G with respect to S is the generating function

$$\Gamma(t) = \sum_{n=0}^{\infty} \gamma(n)t^n$$

Question 8.6.1. Is the function $\Gamma(t)$ rational? Is it algebraic?

It has been suggested to use the recurrence formula derived in this chapter to build a language such that the language growth function coincides with the growth function of F with respect to $\{x_0, x_1\}$ or with the recurrence formula that we have derived. It is known that if a language is regular, the growth series is rational and hence this would be an interesting direction to try. It would be possible to say something even in the case that the language were proved to be context-free or indexed (see [27] for the definitions and the standard results about languages and growth functions).

APPENDIX A

OMITTED PROOFS

A.1 Chapter 2 Appendix: Positive Cochains

Theorem A.1.1. *Let G be a directed graph, and let $c \in H^1(G, \mathbb{Z})$. Suppose that:*

$$c(\ell) \geq 0$$

for every directed cycle ℓ in G . Then c can be represented by a cochain that takes a non-negative value on each directed edge.

We shall prove this statement using a version of the Farkas lemma. Call a vector $v \in \mathbb{R}^n$ *non-negative* if each of its entries is non-negative.

Lemma A.1.2 (Farkas). *Let S be a subspace of \mathbb{R}^n , and let $a \in \mathbb{R}^n$. Then either:*

1. *The affine subspace $a + S$ contains a non-negative vector, or*
2. *There exists a non-negative $v \in S^\perp$ such that $\langle v, a \rangle < 0$. \square*

Figure A.1 illustrates this fact.

Because $a + S$ does not intersect the first quadrant, S^\perp contains a vector v in the first quadrant with $\langle v, a \rangle < 0$. See [64] for more information on the Farkas lemma, including alternate versions and a simple proof.

Proof of Theorem A.1.1: Let E be the set of directed edges in G , and let V be the set of vertices. We will begin by producing a non-negative cocycle in \mathbb{R}^E that represents c .

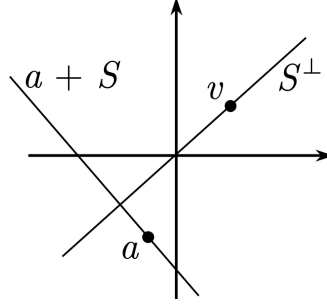


Figure A.1: The Farkas Lemma

The set of all cochains representing c is the affine subspace

$$\alpha + \text{im}(\delta) \subset \mathbb{R}^E$$

where $\alpha \in \mathbb{R}^E$ is any cocycle representing c and $\delta: \mathbb{R}^V \rightarrow \mathbb{R}^E$ is the coboundary map. The orthogonal complement to $\text{im}(\delta)$ is the space of cycles:

$$\text{im}(\delta)^\perp = \ker(\partial)$$

where the boundary map $\partial: \mathbb{R}^E \rightarrow \mathbb{R}^V$ is the adjoint to δ . By hypothesis, $\langle \alpha, \ell \rangle = c(\ell) \geq 0$ for every directed cycle ℓ , and therefore $\langle \alpha, \sigma \rangle \geq 0$ for every positive cycle $\sigma \in \ker(\partial)$. From the Farkas lemma, we conclude that the affine subspace $\alpha + \text{im}(\delta)$ contains a non-negative vector β .

So far, we have proved the existence of a non-negative real cochain β representing c . We wish to modify β to have integer entries. Consider the image cochain $\pi(\beta) \in (\mathbb{R}/\mathbb{Z})^E$. Since $\langle \beta, \ell \rangle = c(\ell) \in \mathbb{Z}$ for any cycle ℓ with integer coefficients, the image $\pi(\beta)$ evaluates to $0 \in \mathbb{R}/\mathbb{Z}$ on any cycle, and is therefore a coboundary. Choose a function $f: V \rightarrow \mathbb{R}/\mathbb{Z}$ so that $\delta f = \pi(\beta)$, and let $\bar{f}: V \rightarrow [0, 1)$ be the lift of f . Then the difference $\beta - \delta \bar{f}$ must have integer entries. Since β is non-negative and $|\left(\delta \bar{f}\right)(e)| < 1$ for any directed edge e , the entries of $\beta - \delta \bar{f}$ must be non-negative integers, and so $\beta - \delta \bar{f}$ is the desired representative for c . \square

A.2 Chapter 4 Appendix: Some Computations

Here is the proof of Proposition 4.4.6:

Proposition A.2.1. *Let $J \subseteq [0, 1]$ be a closed interval with endpoints in S and let $u, v \in J \cap S$. Then $\pi(u) = \pi(v)$ if and only if there is a $g \in \text{PL}_{S,G}(J)$ such that $g(u) = v$.*

Proof. The sufficient condition is implied by Lemma 4.4.5. Suppose now that $J = [\eta, \zeta]$ and let $L = \zeta - \eta$. We recenter the axis at (η, η) , so that interval J is now $[0, L]$. For $\alpha \in G, \beta \in J \cap S$ such that $\alpha\beta < L - \beta$ define (see figure A.2)

$$g_{\alpha,\beta}(t) := \begin{cases} \alpha t & t \in [0, \beta] \\ t - (1 - \alpha)\beta & t \in [\beta, L - \alpha\beta] \\ \frac{1}{\alpha}(t - L) + L & t \in [L - \alpha\beta, L] \end{cases}.$$

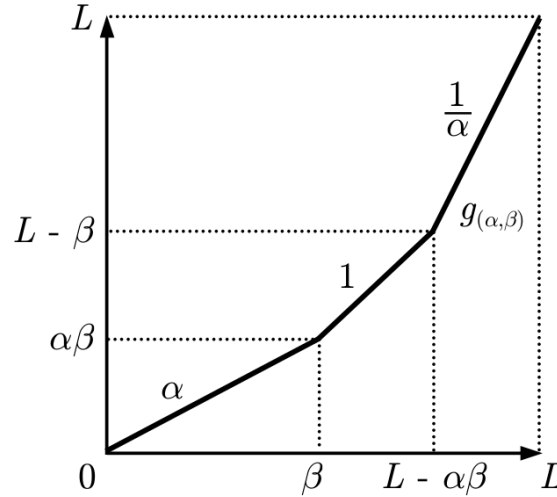


Figure A.2: The basic function to get transitivity.

Using the maps $g_{(\alpha,\beta)}$ or $g_{(\alpha,\beta)}^{-1}$ we can send any number $\beta \leq t \leq L - \alpha\beta$ to $t - (1 - \alpha)\beta$ and any number $\alpha\beta \leq t \leq L - \beta$ to $t + (1 - \alpha)\beta$. We define a relation

on $J \cap S$ by saying that $t_1 \sim t_2$, if either $t_2 = g_{(\alpha,\beta)}(t_1)$ for some $\alpha \in G, \beta \in J \cap S$ such that $\beta \leq t \leq L - \alpha\beta$ or $t_2 = g_{(\alpha,\beta)}^{-1}(t_1)$ for some $\alpha \in G, \beta \in J \cap S$ such that $\alpha\beta \leq t \leq L - \beta$. Then we take the transitive closure of this relation, to get an equivalence relation. Now, since $\pi(u) = \pi(v)$ then we have that $v - u \in \mathcal{I}$ and so

$$v - u = (1 - \alpha_1)\beta_1 + \dots + (1 - \alpha_k)\beta_k$$

for some $\alpha_i \in G, \beta_i \in J \cap S$. We want to rewrite $v - u$ as a sum of terms with β_i 's small enough so that we can use the defined equivalence relation. We will define a suitable sequence of numbers m_i and $\beta_{i,j}$ with $1 \leq j \leq m_i$, for each $i = 1, \dots, k$. Take β_1 and choose a number $\beta_{i,1} \in J \cap S$ small enough such that $g_{(\alpha_i, \beta_{i,1})}$ can be defined. Then choose inductively a number $\beta_{i,j} \in J \cap S$ small enough such that it satisfies all the following three properties

- $g_{(\alpha_i, \beta_{i,j})}$ can be defined
- the number $\beta_{i,j+1}^0 := \beta_i - \beta_{i,1} - \dots - \beta_{i,j} > 0$ is strictly positive
- the number

$$u + (1 - \alpha_1) \sum_{s=1}^{m_1} \beta_{1,s} + \dots + (1 - \alpha_i) \sum_{s=1}^{j-1} \beta_{i,s}$$

lies in the interval $[\beta_{i,j}, L - \alpha_i \beta_{i,j}]$.

We stop when we find an index m_i such that the number β_{i,m_i}^0 has the property that $g_{(\alpha_i, \beta_{i,m_i}^0)}$ can be defined and

$$u + (1 - \alpha_1) \sum_{s=1}^{m_1} \beta_{1,s} + \dots + (1 - \alpha_i) \sum_{s=1}^{m_i-1} \beta_{i,s}$$

lies in the interval $[\beta_{i,m_i}^0, L - \alpha_i \beta_{i,m_i}^0]$ and so we define $\beta_{i,m_i} := \beta_{i,m_i}^0$. We iterate this argument for each $i = 1, \dots, k$ and thus we can rewrite

$$v - u = (1 - \alpha_1) \sum_{j=1}^{m_1} \beta_{1,j} + \dots + (1 - \alpha_k) \sum_{j=1}^{m_k} \beta_{k,j}$$

and so

$$\begin{aligned}
u &\sim u + (1 - \alpha_1)\beta_{1,1} \sim \\
u + (1 - \alpha_1)(\beta_{1,1} + \beta_{1,2}) &\sim \dots \sim \\
u + (1 - \alpha_1) \sum_{j=1}^{m_1} \beta_{1,j} &\sim \dots \sim \\
u + (1 - \alpha_1) \sum_{j=1}^{m_1} \beta_{1,j} + \dots + (1 - \alpha_k) \sum_{j=1}^{m_k} \beta_{k,j} &= v
\end{aligned}$$

implying that there exists an element $g \in \text{PL}_{S,G}(J)$ such that $g(u) = v$. \square

BIBLIOGRAPHY

- [1] V. S. Afraimovich and T. Young. Mather invariants and smooth conjugacy on S^2 . *J. Dynam. Control Systems*, 6(3):341–352, 2000.
- [2] I. Anshel, M. Anshel, and D. Goldfeld. An algebraic method for public-key cryptography. *Math. Res. Lett.*, 6(3-4):287–291, 1999.
- [3] G. R. Belitskiĭ. Smooth classification of one-dimensional diffeomorphisms with hyperbolic fixed points. *Sibirsk. Mat. Zh.*, 27(6):21–24, 1986.
- [4] James M. Belk and Kenneth S. Brown. Forest diagrams for elements of Thompson’s group F . *Internat. J. Algebra Comput.*, 15(5-6):815–850, 2005.
- [5] J.M. Belk. *Thompson’s Group F* . PhD thesis, Cornell University, 2004. [arXiv:math.GR/0708.3609v1](#).
- [6] J.M. Belk and F. Matucci. Conjugacy in thompson’s groups. *preprint*. [arXiv:math.GR/0708.4250v1](#).
- [7] J.M. Belk and F. Matucci. Dynamics in thompson’s group f . *preprint*. [arXiv:math.GR/0710.3633v1](#).
- [8] C. Bleak and D. Farley. Private communication.
- [9] Collin Bleak. *Solvability in Groups of Piecewise-linear Homeomorphisms of the Unit Interval*. PhD thesis, Binghamton University, 2005. [arXiv:math.GR/0708.3609v1](#).
- [10] W. A. Bogley and S. J. Pride. Calculating generators of Π_2 . In *Two-dimensional homotopy and combinatorial group theory*, volume 197 of *London Math. Soc. Lecture Note Ser.*, pages 157–188. Cambridge Univ. Press, Cambridge, 1993.
- [11] O. Bogopolski, A. Martino, O. Maslakova, and E. Ventura. The conjugacy problem is solvable in free-by-cyclic groups. *Bull. London Math. Soc.*, 38(5):787–794, 2006.
- [12] O. Bogopolski, A. Martino, and E. Ventura. Orbit decidability and the conjugacy problem for some extensions of groups. *preprint*. [arXiv:math.GR/0712.3104v1](#).

- [13] Martin R. Bridson and James Howie. Conjugacy of finite subsets in hyperbolic groups. *Internat. J. Algebra Comput.*, 15(4):725–756, 2005.
- [14] Matthew G. Brin. The chameleon groups of Richard J. Thompson: automorphisms and dynamics. *Inst. Hautes Études Sci. Publ. Math.*, (84):5–33 (1997), 1996.
- [15] Matthew G. Brin. Higher dimensional Thompson groups. *Geom. Dedicata*, 108:163–192, 2004.
- [16] Matthew G. Brin. On the Zappa-Szép product. *Comm. Algebra*, 33(2):393–424, 2005.
- [17] Matthew G. Brin. The algebra of strand splitting. I. A braided version of Thompson’s group V . *J. Group Theory*, 10(6):757–788, 2007.
- [18] Matthew G. Brin and Craig C. Squier. Groups of piecewise linear homeomorphisms of the real line. *Invent. Math.*, 79(3):485–498, 1985.
- [19] Matthew G. Brin and Craig C. Squier. Presentations, conjugacy, roots, and centralizers in groups of piecewise linear homeomorphisms of the real line. *Comm. Algebra*, 29(10):4557–4596, 2001.
- [20] Kenneth S. Brown. *Cohomology of groups*, volume 87 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. Corrected reprint of the 1982 original.
- [21] J. Burillo, C. Cleary, M. Stein, and T. Taback. Combinatorial and metric properties of Thompson’s group t . *Transactions of the AMS*. to appear, arXiv:math.GR/0607167v2.
- [22] J. Burillo and Cleary. S. Metric properties in the braided Thompson’s groups. *Indiana University Mathematics Journal*. to appear, arXiv:math.GR/0710.5518v1.
- [23] José Burillo. Growth of positive words in Thompson’s group F . *Comm. Algebra*, 32(8):3087–3094, 2004.
- [24] Danny Calegari. Denominator bounds in Thompson-like groups and flows. *Groups Geom. Dyn.*, 1(2):101–109, 2007.

- [25] J.W. Cannon, W.J. Floyd, and W.R. Parry. Introductory notes on Richard Thompson's groups. *Enseign. Math.* (2), 42(3-4):215–256, 1996.
- [26] Pierre de la Harpe. *Topics in geometric group theory*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 2000.
- [27] David B. A. Epstein, James W. Cannon, Derek F. Holt, Silvio V. F. Levy, Michael S. Paterson, and William P. Thurston. *Word processing in groups*. Jones and Bartlett Publishers, Boston, MA, 1992.
- [28] Benson Farb and John Franks. Groups of homeomorphisms of one-manifolds. III. Nilpotent subgroups. *Ergodic Theory Dynam. Systems*, 23(5):1467–1484, 2003.
- [29] Benson Farb and Peter Shalen. Groups of real-analytic diffeomorphisms of the circle. *Ergodic Theory Dynam. Systems*, 22(3):835–844, 2002.
- [30] S. Blake Fordham. Minimal length elements of Thompson's group F . *Geom. Dedicata*, 99:179–220, 2003.
- [31] Étienne Ghys and Vlad Sergiescu. Sur un groupe remarquable de difféomorphismes du cercle. *Comment. Math. Helv.*, 62(2):185–239, 1987.
- [32] N. Gill and I. Short. Conjugacy in thompson's group. *preprint*. [arXiv:math.GR/0709.1987v2](https://arxiv.org/abs/math.GR/0709.1987v2).
- [33] S. Goldwasser and M. Bellare. *Lecture Notes on Cryptography*. 2001. <http://www.cse.ucsd.edu/users/mihir/papers/gb.pdf>.
- [34] R. I. Grigorchuk, V. V. Nekrashevich, and V. I. Sushchanskiĭ. Automata, dynamical systems, and groups. *Tr. Mat. Inst. Steklova*, 231(Din. Sist., Avtom. i Beskon. Gruppy):134–214, 2000.
- [35] Fritz Grunewald and Daniel Segal. Some general algorithms. I. Arithmetic groups. *Ann. of Math.* (2), 112(3):531–583, 1980.
- [36] V. S. Guba. On the properties of the Cayley graph of Richard Thompson's group F . *Internat. J. Algebra Comput.*, 14(5-6):677–702, 2004. International Conference on Semigroups and Groups in honor of the 65th birthday of Prof. John Rhodes.

- [37] V. S. Guba and M. V. Sapir. On subgroups of the R. Thompson group F and other diagram groups. *Mat. Sb.*, 190(8):3–60, 1999.
- [38] Victor Guba and Mark Sapir. Diagram groups. *Mem. Amer. Math. Soc.*, 130(620):viii+117, 1997.
- [39] Michael-Robert Herman. Sur la conjugaison différentiable des difféomorphismes du cercle à des rotations. *Inst. Hautes Études Sci. Publ. Math.*, (49):5–233, 1979.
- [40] Graham Higman. *Finitely presented infinite simple groups*. Department of Pure Mathematics, Department of Mathematics, I.A.S. Australian National University, Canberra, 1974. Notes on Pure Mathematics, No. 8 (1974).
- [41] J. E. Hopcroft and J. K. Wong. Linear time algorithm for isomorphism of planar graphs: preliminary report. In *Sixth Annual ACM Symposium on Theory of Computing (Seattle, Wash., 1974)*, pages 172–184. Assoc. Comput. Mach., New York, 1974.
- [42] M. Kassabov and F. Matucci. The simultaneous conjugacy problem in groups of piecewise linear functions. *preprint*. arXiv:math.GR/0607167v2.
- [43] V. Kilibarda. *On the algebra of semigroup diagrams*. PhD thesis, University of Nebraska, 1994.
- [44] K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J. Kang, and C. Park. New public-key cryptosystem using braid groups. In *Advances in cryptology—CRYPTO 2000 (Santa Barbara, CA)*, volume 1880 of *Lecture Notes in Comput. Sci.*, pages 166–183. Springer, Berlin, 2000.
- [45] R. S. MacKay. A simple proof of Denjoy’s theorem. *Math. Proc. Cambridge Philos. Soc.*, 103(2):299–303, 1988.
- [46] Paul Malliavin. *Integration and probability*, volume 157 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With the collaboration of Hélène Airault, Leslie Kay and Gérard Letac, Edited and translated from the French by Kay, With a foreword by Mark Pinsky.
- [47] Gregory Margulis. Free subgroups of the homeomorphism group of the circle. *C. R. Acad. Sci. Paris Sér. I Math.*, 331(9):669–674, 2000.

- [48] John N. Mather. Commutators of diffeomorphisms. *Comment. Math. Helv.*, 49:512–528, 1974.
- [49] F. Matucci. Cryptanalysis of the Shpilrain-Ushakov protocol for Thompson’s group. *Journal of Cryptology*, 21(3):458–468. arXiv:math.GR/0607184v1.
- [50] M. H. A. Newman. On theories with a combinatorial definition of “equivalence.”. *Ann. of Math. (2)*, 43:223–243, 1942.
- [51] J. F. Plante and W. P. Thurston. Polynomial growth in holonomy groups of foliations. *Comment. Math. Helv.*, 51(4):567–584, 1976.
- [52] Stephen J. Pride. Geometric methods in combinatorial semigroup theory. In *Semigroups, formal languages and groups (York, 1993)*, volume 466 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 215–232. Kluwer Acad. Publ., Dordrecht, 1995.
- [53] Stephen J. Pride. Low-dimensional homotopy theory for monoids. *Internat. J. Algebra Comput.*, 5(6):631–649, 1995.
- [54] Alain M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.
- [55] Derek J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.
- [56] D. Ruinskiy, A. Shamir, and B. Tsaban. Length-based cryptanalysis: The case of Thompson’s group. *Journal of Mathematical Cryptology*. to appear, arXiv:cs/0607079v4.
- [57] D. Ruinskiy, A. Shamir, and B. Tsaban. Cryptanalysis of group-based key agreement protocols using subgroup distance functions. In *Proceedings of the 10th International Conference on Practice and Theory in Public-Key Cryptography PKC07*, volume 4450 of *Lecture Notes in Comput. Sci.*, pages 61–75. 2007.
- [58] Olga Salazar-Díaz. *Thompson’s group V from the dynamical viewpoint*. PhD thesis, State University of New York at Binghamton, 2006.
- [59] R. A. Sarkisyan. The conjugacy problem for collections of integral matrices. *Mat. Zametki*, 25(6):811–824, 956, 1979.

- [60] Elizabeth A. Scott. A finitely presented simple group with unsolvable conjugacy problem. *J. Algebra*, 90(2):333–353, 1984.
- [61] V Shpilrain and A. Ushakov. Thompson’s group and public key cryptography. In *ACNS 2005*, volume 3531 of *Lecture Notes in Comput. Sci.*, pages 151–163. 2005.
- [62] Jean-Christophe Yoccoz. Centralisateurs et conjugaison différentiable des difféomorphismes du cercle. *Astérisque*, (231):89–242, 1995. Petits diviseurs en dimension 1.
- [63] Todd R. Young. C^k conjugacy of 1-D diffeomorphisms with periodic points. *Proc. Amer. Math. Soc.*, 125(7):1987–1995, 1997.
- [64] Günter M. Ziegler. *Lectures on polytopes*, volume 152 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.